Tentamen i TDDC75 Diskreta strukturer

2016-10-27, kl. 8–13

- Ta det lugnt, arbeta metodiskt, kolla dina svar.
- Kom ihåg att svaren på samtliga uppgifter måste **motiveras**, och att motiveringarna skall vara uppställda på ett sådant sätt att det går att följa hur du har tänkt. *Omotiverade svar ger 0 poäng om inget annat sägs.*
- Maxpoäng är 30 poäng. För betyg 3 krävs minst 15 poäng, för betyg 4 krävs 20 poäng och för betyg 5 krävs 25 poäng.

Lycka till!!!

1. Betrakta följande satslogiska uttryck: $(p \vee q) \wedge (\neg p \vee \neg q)$

   (a) Skapa en sanningstabell för uttrycket.

   (b) Visa genom deduktion att $(p \vee q) \wedge (\neg p \vee \neg q) \models \neg p \leftrightarrow q$. Använd endast lagarna i formelbladet sist i tentan.

   (c) Gäller även det omvända, d.v.s. $\neg p \leftrightarrow q \models (p \vee q) \wedge (\neg p \vee \neg q)$? Visa eller motbevisa (valfri metod).

   (5 poäng)

2. Låt F vara mängden av alla filer på en hårddisk. Låt f_1, f_2 och f_3 vara tre olika filer på hårddisken (och alltså element i F). Avgör om följande påståenden är sanna, falska eller om det saknas tillräcklig information för att avgöra. (Som alltid, motivera dina svar.)

   (a) $\{f_1\} \in F$

   (b) $\{f_1\} \subset F$

   (c) $\{f_1, f_2\} \subseteq (F \cap \{f_3\})$

   (d) $\{f_1, f_2\} \subseteq 2^F$

   (e) $|2^A| \leq |2^B|$ där $A = \{f_1, f_3\}$ och $B = F \setminus \{f_1, f_2\}$

   (5 poäng)

3. Vi börjar med att rekapitulera ett par definitioner. Sammansättningen av två relationer $R \subseteq A \times B$ och $S \subseteq B \times C$ definieras som

$$S \circ R = \{(x, z) \mid \exists y \in B[(x, y) \in R \wedge (y, z) \in S]\}$$

Vidare, om $R \subseteq A \times A$ kan vi definiera

$$\begin{array}{lcll} R^0 & = & id_A & \\ R^{n+1} & = & R \circ R^n & (n \geq 0) \end{array}$$

Visa med hjälp av induktion att om R är symmetrisk så är även R^n symmetrisk för alla $n \geq 0$.

(5 poäng)

4. 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?

(5 poäng)

5. Låt A, B, C vara godtyckliga mängder. Visa att om $A \cup B = A \cup C$ och $\overline{A} \cup B = \overline{A} \cup C$ så måste $B = C$.

(5 poäng)

6. Betrakta en sorts enkelt datorprogram bestående av endast tilldelningssatser med primitiva variabeltyper (inga loopar, villkorssatser, eller funktioner). Ett exempel på ett sådant program visas nedan (radnumret anges i parentes).

   (1) $a = 1$
   (2) $b = a$
   (3) $c = 5$
   (4) $d = b + c$
   (5) $e = b - (a * c)$

   Låt $V = \{v_1, \ldots, v_n\}$ vara en mängden med alla variabelnamn för ett visst program P bestående av m rader. Låt relationen $T_i \subseteq V \times V$ bestå av variabelpar (v_v, v_h) sådana att v_v förekommer på vänster sida av tilldelningen på rad i, och v_h förekommer på höger sida på samma rad (för varje rad i finns endast en variabel på vänster sida). I exemplet ovan skulle till exempel $T_4 = \{(d, b), (d, c)\}$

   Låt relationen $R \subseteq V \times V$ definieras som

   $$R_0 = id_V$$

   $$R_i = (R_{i-1} \circ T_i) \cup R_{i-1} \text{ för } i \geq 1$$

   $$R = R_m$$

   (a) Är R alltid, aldrig eller ibland en partialordning?

   (b) Låt $v \in V$ vara en variabel. Tolka påståendet

   $$(v_d, v) \in R \rightarrow (v_d = v)$$

   i relation till programmet P.

   (c) Låt $E = (R \cup R^{-1})^+$, alltså det transitiva höljet av det symmetriska höljet av R. Vad är innebörden av påståendet

   $$(v_1, v_2) \notin E$$

   för två variabler v_1 och v_2? Vad innebär det för möjligheten att ändra ordningen på två programrader i och j som tilldelar värden till v_1 respektive v_2?

(5 poäng)

A Formelblad

Regel	**Benämning**
$\neg\neg p \equiv p$	Lagen om dubbel negation
$\neg(p \wedge q) \equiv (\neg p \vee \neg q)$ $\neg(p \vee q) \equiv (\neg p \wedge \neg q)$	De Morgans lagar
$(p \wedge (q \wedge r)) \equiv ((p \wedge q) \wedge r)$ $(p \vee (q \vee r)) \equiv ((p \vee q) \vee r)$	Associativa lagarna
$(p \wedge (q \vee r)) \equiv ((p \wedge q) \vee (p \wedge r))$ $(p \vee (q \wedge r)) \equiv ((p \vee q) \wedge (p \vee r))$	Distributiva lagarna
$(p \wedge p) \equiv p$ $(p \vee p) \equiv p$	Idempotens
$(p \wedge 1) \equiv p$ $(p \vee 0) \equiv p$	Identitetslagarna
$(p \wedge 0) \equiv 0$ $(p \vee 1) \equiv 1$	Dominans
$(p \wedge \neg p) \equiv 0$ $(p \vee \neg p) \equiv 1$	Inversa lagarna
$(p \wedge (p \vee q)) \equiv p$ $(p \vee (p \wedge q)) \equiv p$	Absorption
$(p \to q) \equiv (\neg p \vee q)$	Implikationslagen
$(p \to q) \equiv (\neg q \to \neg p)$	Kontrapositiva lagen
$(p \leftrightarrow q) \equiv ((p \to q) \wedge (q \to p))$	Ekvivalenslagen
$(p \to q), p \models q$	Modus ponens
$(p \to q), \neg q \models \neg p$	Modus tollens
$(p \to q), (q \to r) \models p \to r$	Syllogism
$p \wedge q \models p$	Konjunktiv förenkling
$p \models p \vee q$	Disjunktiv förstärkning
$(p \vee q), \neg q \models p$	Disjunktiv syllogism
$p, q \models p \wedge q$	Konjunktionsregeln

Tabell 1: Logiska ekvivalenser och konsekvenser