Försättsblad till skriftlig tentamen vid Linköpings universitet

Datum för tentamen	2019-10-22
Sal (2)	U3(20) U4(20)
Tid	8-12
Utb. kod	TDDC75
Modul	TEN2
Utb. kodnamn/benämning **Modulnamn/benämning**	Diskreta strukturer En skriftlig tentamen
Institution	IDA
Antal uppgifter som ingår i tentamen	6
Jour/Kursansvarig Ange vem som besöker salen	Mikael Asplund
Telefon under skrivtiden	0700 895 827
Besöker salen ca klockan	9-10
Kursadministratör/kontaktperson (namn + tfnr + mailaddress)	Veronica Kindeland Gunnarsson veronica.kindeland.gunnarsson@liu.se 013-28 56 34
Tillåtna hjälpmedel	Inga
Övrigt	
Antal exemplar i påsen	

Försättsblad till skriftlig tentamen vid Linköpings universitet

Datum för tentamen	2019-10-22
Sal (2)	U3(20) U4(20)
Tid	8-12
Utb. kod	TDDC75
Modul	TEN2
Utb. kodnamn/benämning **Modulnamn/benämning**	Diskreta strukturer En skriftlig tentamen
Institution	IDA
Antal uppgifter som ingår i tentamen	6
Jour/Kursansvarig Ange vem som besöker salen	Mikael Asplund
Telefon under skrivtiden	0700 895 827
Besöker salen ca klockan	9-10
Kursadministratör/kontaktperson (namn + tfnr + mailaddress)	Veronica Kindeland Gunnarsson veronica.kindeland.gunnarsson@liu.se 013-28 56 34
Tillåtna hjälpmedel	Inga
Övrigt	
Antal exemplar i påsen	

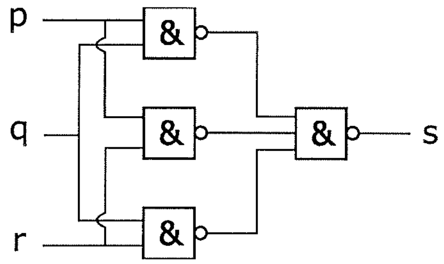
Tentamen i TDDC75 Diskreta strukturer

2019-10-22

- Ta det lugnt, arbeta metodiskt, kolla dina svar.
- Om du misstänker fel i någon uppgift kontakta jourlärare, Mikael Asplund, 0700 895 827.
- 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. I säkerhetskritiska tillämpningar (flygplan, kärnkraftverk, osv) används ofta konceptet Triple Modular Redundancy (TMR) vilket innebär att tre moduler med identisk funktionalitet implementeras och utdatat från de tre modulerna jämförs och majoritetsröstning avgör vad det slutliga utresultatet blir. I figuren nedan visas hur en sådan röstningskrets kan konstrueras för en bit med hjälp av NAND-grindar.



Vi kan uttrycka sambandet mellan de ingående variablerna på följande vis,

$$s \leftrightarrow \neg(\neg(p \wedge q) \wedge \neg(p \wedge r) \wedge \neg(q \wedge r)).$$

(a) Skriv om uttrycket ovan så att det inte innehåller några negationer ($\neg$). (1p)

(b) Låt F beteckna uttrycket från uppgift a) och använd satslogisk deduktion och de regler om finns i formelbladet sist i tentan för att visa följande påstående.

$$p, s, F \Rightarrow q \vee r$$

Tips: använd motsägelsebevis (indirekt härledning). (4p)

(5 poäng)

2. Betrakta följande mängder.

   - $A = \{0, 1\}$
   - $B = \{0, 1, 2\}$
   - $C = \{\varnothing\}$
   - $D = \varnothing$

   Ange vilka mängder som betecknas med uttrycken nedan.

   (a) $A \cup (B \setminus C)$

   (b) $2^{B \setminus A}$

   (c) $(A \cup C) \cap 2^B$

   (d) $2^C \cap 2^D$

   (e) $(C \cup D) \times A$

(5 poäng)

3. Låt mängden A beteckna alla svenska registreringsskyltar på som har formen ABC123 eller ABC12D (den nya varianten). Låt relationen $R \subseteq A \times A$ vara definierad så att $(x, y) \in R$ omm registreringsskyltarna x och y skiljer sig åt på exakt ett ställe. Till exempel gäller att $(ABC123, AXC123) \in R$ eftersom andra tecknet skiljer sig åt. Förklara varför eller varför inte R är:

   - Reflexiv, och om inte, beskriv det reflexiva höljet av R.
   - Transitiv, och om inte, beskriv det transitiva höljet av R.
   - Symmetrisk och om inte, beskriv det symmetriska höljet av R:
   - Anti-symmetrisk

(5 poäng)

4. I så kallade blockkedjor så länkas informationen i olika datablock samman med hjälp av hashfunktioner. En hashfunktion kan beskrivas som en funktion $f : A \to B$ där mängden A innehåller element av varierande storlek (till exempel innehållet i en fil, eller ett block) och B består av bitsträngar av en viss längd. I blockkedjor (och andra sammanhang där man använder kryptografiska hashfunktioner) är det viktigt att givet ett visst element $y \in B$ så ska det vara svårt att finna ett $x \in A$ sådant att $f(x) = y$.

   Generellt så gäller att $|A| >> |B|$, det vill säga det finns många fler element i definitionsmängden än i målmängden för en hashfunktion.

   (a) Är det då möjligt för en hashfunktion att vara injektiv? (1p)

   (b) Är det då möjligt för en hashfunktion att vara surjektiv? (1p)

   (c) Låt A vara en mängd med n element och B_k mängden av alla bitsträngar av längden k. Så till exempel är $010 \in B_3$. Låt F_k vara mängden av alla funktioner från A till B_k. Hur många element finns i mängden F_k? (3p)

   (5 poäng)

5. Bevisa att följande påstående gäller för alla heltal $n \geq 1$.

$$1 + 3 + 5 + \ldots + (2n - 1) = n^2$$

   (5 poäng)

6. Låt Γ vara en godtycklig mängd satslogiska formler.

   (a) Förklara innebörden av påståendet $\Gamma \not\Rightarrow F \to G$ med hjälp av definitionen av logisk konsekvens så som den har definierats på föreläsningen (dvs i termer av sanningsvärden i olika tolkningar). (1.5p)

   (b) Visa att om $\Gamma \not\Rightarrow F \to G$ (alltså att $F \to G$ inte är en logisk konsekvens av formlerna i Γ) så gäller att $\Gamma, F \not\Rightarrow G$ för godtyckliga satslogiska formler F och G. (3.5p)

   (5 poäng)

A Formelblad

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

Tabell 1: Logiska ekvivalenser och konsekvenser