

Formal Verification and Specification
Final Exam
June 06, 2022

True/False

(03 points) Write True if the statement is true, otherwise write False.

- _____ Linkage variable in Method-B is used for linking two sets
- _____ pUq is true if p is false in the current state and q is true
- _____ It is not possible to implement an abstract machine without passing by the refinement step
- _____ SPIN is a language used in model checking
- _____ Every LTL property might be translated into Buchi automaton
- _____ $AGAFp \equiv AGFp$

Section 2. Set theory(04 points)

1. We have three sets and two relations as presented in the Figure 1. We have a set of **teachers** (first set), who own (R1) a set of **datashows** (second set). Each datashow *has* (R2) possible **options**(third set). Introduce the following:

- Domain: $\text{dom}(R2)$
- Range: $\text{range}(R1)$
- Domain restriction: $U < |R1 : U = \text{Hichem}$
- Domain anti-restriction: $U < |R1 : U = \text{Hichem, Leila}$
- Range restriction: $R1| > U : U = \text{Condor}$

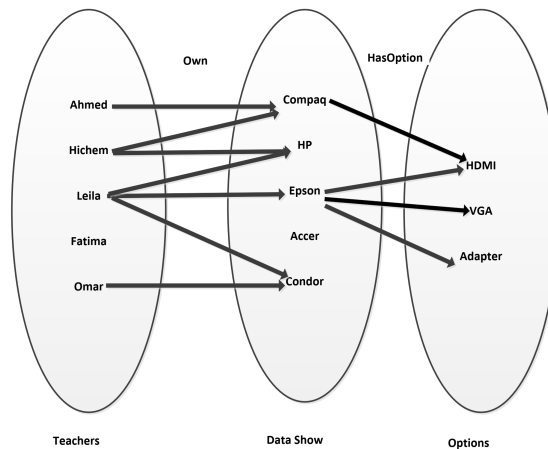


Figure 1: Sets and relations

Section 3. Method-B Specification(06 points)

2. Suppose that we have the following problem: The computer science department has a number of available *Datashows*, and each one has possible *options* such as HDMI, VGA, ... A teacher may perform three main operations of the requested DataShow:

- **Add:** add an option to the requested datashow
- **Remove:** Remove an option from the requested datashow
- **HasOption:** Asks whether the requested datashow is allowed to include a specific option

We consider the following:

- Three main sets: *Datashows*, *OPTION* and *Allowed* =OK, KO.
- One relation *options* from *Datashows* to *OPTION*.

Where the relation is denoted by $\langle - \rangle$ and a pair or a Maplet is denoted by $| - \rangle$.

Section 4. ω -expressions(03 points)

3. Give the ω -regular expressions for the following buchi automaton :

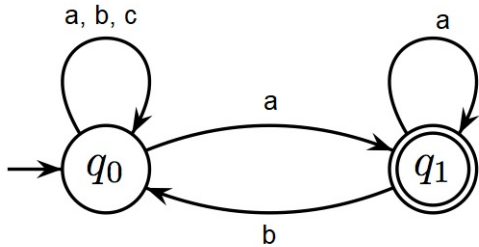


Figure 2: Automate one.

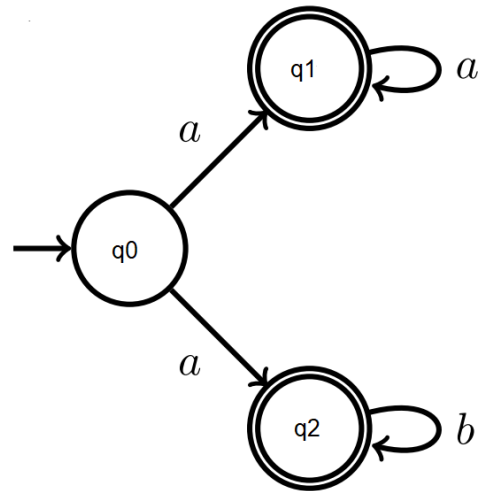


Figure 3: Automate two.

Section 5. LTL Specification(04 points)

4. express in LTL the following properties

- p is true again and again
- From somepoint and on, either you see $\neg a$ now, or in the next step.
- The drink is served once the tokens reach the required number and the drinks is available

Answer Key for Exam A

True/False

(03 points) Write True if the statement is true, otherwise write False.

- False Linkage variable in Method-B is used for linking two sets
- True pUq is true if p is false in the current state and q is true
- False It is not possible to implement an abstract machine without passing by the refinement step
- False SPIN is a language used in model checking
- True Every LTL property might be translated into Buchi automaton
- False $AGAFp \equiv AGFp$

Section 2. Set theory(04 points)

1. We have three sets and two relations as presented in the Figure 1. We have a set of **teachers** (first set), who own (R1) a set of **datashows** (second set). Each datashow *has* (R2) possible **options**(third set). Introduce the following:

- Domain: $\text{dom}(R2)$
- Range: $\text{range}(R1)$
- Domain restriction: $U < |R1 : U = \text{Hichem}$
- Domain anti-restriction: $U < |R1 : U = \text{Hichem, Leila}$
- Range restriction: $R1 | > U : U = \text{Condor}$

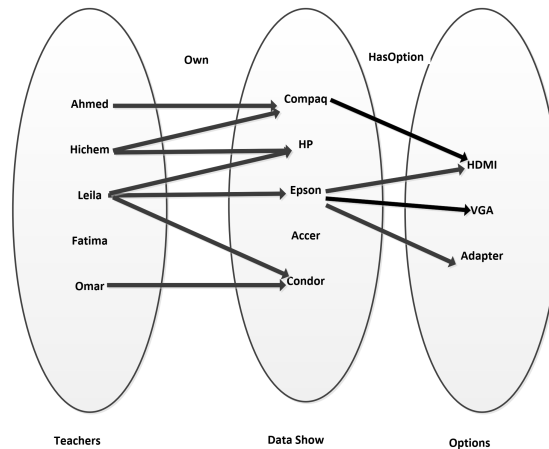


Figure 4: Sets and relations

- Answer:**
- Domain restriction: $U < |R1 : U = \text{Hichem} : \text{Hichem-}_i\text{HP, Hichem-}_i\text{Compaq}$
 - Domain anti-restriction: $U < |R1 : U = \text{Hichem, Leila} : \text{Ahmed-}_i\text{Compaq, Omar-}_i\text{Condor}$
 - Range restriction: $R1 | > U : U = \text{Condor} : \text{Leila-}_i\text{Condor, Omar-}_i\text{Condor}$

Section 3. Method-B Specification(06 points)

2. Suppose that we have the following problem: The computer science department has a number of available *Datashows*, and each one has possible *options* such as HDMI, VGA, ... A teacher may perform three main operations of the requested DataShow:

- **Add:** add an option to the requested datashow
- **Remove:** Remove an option from the requested datashow
- **HasOption:** Asks whether the requested datashow is allowed to include a specific option

We consider the following:

- Three main sets: *Datashows*, *OPTION* and *Allowed* =OK, KO.
- One relation *options* from *Datashows* to *OPTION*.

Where the relation is denoted by $\langle - \rangle$ and a pair or a Maplet is denoted by $| - \rangle$.

Answer:

Section 4. ω -expressions(03 points)

3. Give the ω -regular expressions for the following buchi automaton :

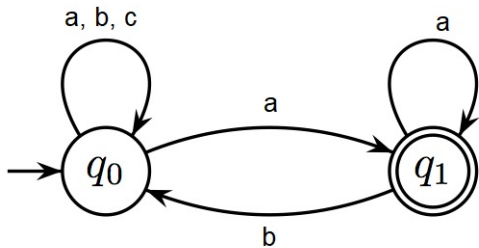


Figure 5: Automate one.

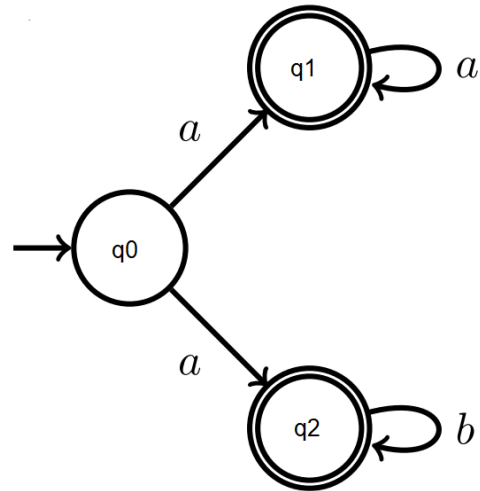


Figure 6: Automate two.

- Answer:**
- $(a + b + c)(a + ab)^\omega$
 - $a^\omega + ab^\omega$

Section 5. LTL Specification(04 points)

4. express in LTL the following properties

- p is true again and again
- From somepoint and on, either you see $\neg a$ now, or in the next step.

- The drink is served once the tokens reach the required number and the drinks is available

Answer: • GFp

- $FG(\neg a \vee X\neg a)$
- $(drink_a \text{ available} \wedge \neg tokens) \text{ U served}$