CPSC 406

Tyler Lewis
Chapman University

April 16, 2023

Abstract

A very short introduction to typesetting in LaTeX for my courses "Programming Languages", "Compiler Construction" and "Algorithm Analysis".

Contents

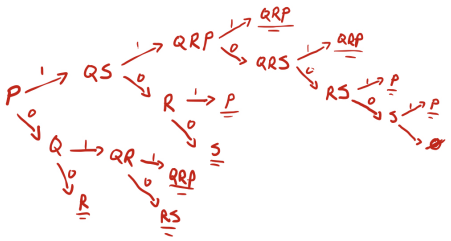
1 Homework **1**
1.1 HW 1 . . . 1
1.2 HW 2 . . . 2
1.3 HW 6 . . . 4
1.4 HW 9 . . . 5

2 Conclusions **6**

1 Homework

1.1 HW 1

NFA2DFA In order to convert the provided NFA to DFA I considered each possible combination of P, Q, R, and S, and considered each possible combination its own state. The included figure details every possible state the NFA/DFA may find itself in.



state	0	1
P	Q	QS
R	S	P
Q	R	QR
S	Ø	P
QS	R	QRP
QR	RS	QRP
RS	S	P
QRP	QRS	QRP
QRS	RS	QRP

1.2 HW 2

Question 1:

1. $f(X, f(X,Y)) \stackrel{?}{=} f(f(Y,a), f(U,b))$

$X \stackrel{?}{=} f(Y,a)$ $\quad f(X,Y) \stackrel{?}{=} f(U,b)$

$\sigma_1 = \frac{f(Y,a)}{X}$ $\quad X = U$ $\quad Y = b$

$\sigma_2 = \frac{U}{X}$ $\quad \sigma_3 = \frac{b}{Y}$

$\sigma = \left[\frac{f(Y,a)}{X}, \frac{U}{X}, \frac{b}{U}\right]$

2. $f(g(U), f(X,Y)) \stackrel{?}{=} f(X, f(Y,U))$

$g(U) \stackrel{?}{=} X$ $\quad f(X,Y) \stackrel{?}{=} f(Y,U)$

$X \stackrel{?}{=} Y$ $\quad Y \stackrel{?}{=} U$

$X \stackrel{?}{=} U$

$\sigma = \frac{g(X)}{X}$ Fail

3. $h(U, f(g(V), W), g(W)) \stackrel{?}{=} h(f(X,b), U, Z)$

$U \stackrel{?}{=} f(X,b)$ $\quad f(g(V), W) \stackrel{?}{=} U$ $\quad g(W) \stackrel{?}{=} Z$

$f(g(V), W) \stackrel{?}{=} f(X,b)$ $\quad \sigma_3 = \frac{g(W)}{Z}$

$g(V) \stackrel{?}{=} X$ $\quad W \stackrel{?}{=} b$

$\sigma_1 = \frac{g(V)}{X}$ $\quad \sigma_2 = \frac{b}{W}$

$\sigma = \sigma_1 \circ \sigma_2 \circ \sigma_3 = \left[\frac{g(V)}{X}, \frac{b}{W}, \frac{g(W)}{Z}\right]$

Question 2:

?- conn(W,a), conn(a,W)

?- addr(W,a), addr(a,Z), serv(Z), addr(Z,W) `?- twoway(W,a)`

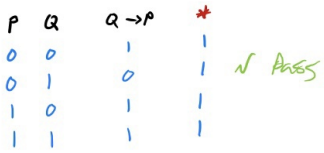
```
?- conn(W,a), conn(a,W)
?- addr(W,a), addr(a,Z), serv(Z), addr(Z,W)
```

1.3 HW 6

1. $P \vee \neg P$

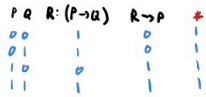
2. $(P \to Q) \to (\neg Q \to \neg P)$

3. $P \to (Q \to P)$



4. $(P \to Q) \vee (Q \to P)$

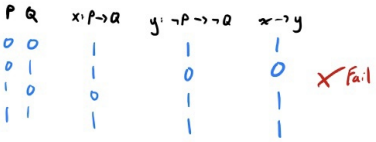
5. $((P \to Q) \to P) \to P$



6. $(P \vee Q) \wedge (\neg P \vee R) \to Q \vee R$

7. $(P \vee Q) \to (P \wedge Q)$

8. $(P \to Q) \to (\neg P \to \neg Q)$



1.4 HW 9

HackMD Page

Exercise 1:

- ‘success‘: This is a propositional variable that is true if both statusA and statusB are ok. This variable is used to check whether the protocol was executed successfully.
- ‘aliceBob‘: This is a propositional variable that is true if ‘partnerA‘ is ‘bob‘. This variable is used to check whether Alice successfully communicated with Bob.
- ‘bobAlice‘: This is a propositional variable that is true if ‘partnerB‘ is ‘alice‘. This variable is used to check whether Bob successfully communicated with Alice.
- ‘&&‘: This is the logical AND operator. It is used to combine two boolean expressions and evaluate to true if both expressions are true.
- ‘→‘: This is the implication operator. It is used to specify a condition that must be satisfied in order for an action to occur. For example, in the statement ‘(data.key == keyA) && (data.d1 == nonceA) →‘, the action on the right-hand side can only occur if the conditions on the left-hand side are true.
- ‘[]‘: This is the "always" operator. It is used to specify a condition that must always be true in order for a property to hold. For example, the property $[](success \rightarrow (aliceBob \wedge bobAlice))$ specifies that if the protocol was executed successfully, then Alice must have communicated with Bob and Bob must have communicated with Alice.
- ‘[]A‘: This is the "always eventually" operator. It is used to specify a condition that must eventually be true in order for a property to hold.

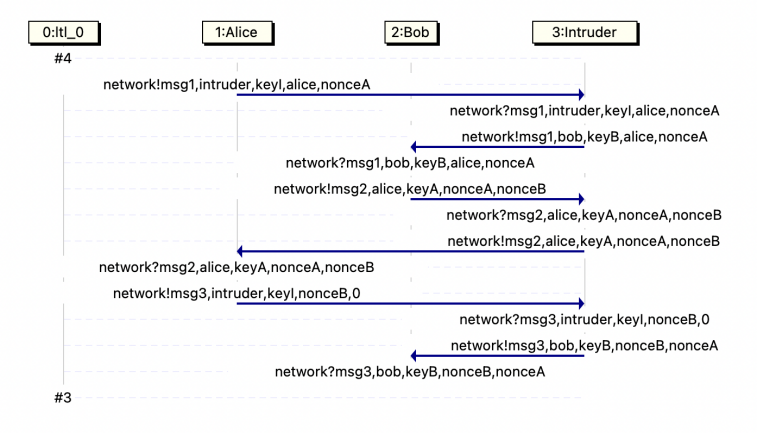
Exercise 2:

The first formula, ’ltl [] (success && aliceBob -> bobAlice) is not violated’, is verified as correct, meaning that the property holds for all possible executions of the protocol. However, the second formula, ’ltl [] (success && bobAlice -> aliceBob) is violated’, is not correct, meaning that there exists at least one execution of the protocol where the property does not hold.

Exercise 3:

The property that is violated produces an execution sequence where the specified property does not hold. Based on the trail file, the length of the execution sequence that violated the property is 84 steps. This is the total number of steps taken during the execution of the protocol before the assertion was violated.

Exercise 4:



The attack was successful because the intruder was able to intercept the messages exchanged between Alice and Bob and alter them in such a way that Alice believed she was communicating with Bob when in fact she was communicating with the intruder. Specifically, the intruder was able to send messages to Alice and sign them with Bob's key, thereby convincing Alice that she was receiving messages from Bob when in fact they were coming from the intruder.

2 Conclusions

In this document, to help you getting started, I gave a first succinct example of typesetting in Latex.

References

[ALG] Algorithm Analysis, Chapman University, 2023.