Homework Week01

Circularity (1 mark)

What is the answer to this question?

Answer:

Leslie Lamport's pants

Dining Cryptographers (2 marks)

Assume the setting described in the first lecture for the problem of the Dining Cryptographers. Suppose we modify the protocol so that paying cryptographers now tell the truth about whether the coin tosses are different or equal. Instead, they will lie about whether they got head or tails.

At the end, do we still know if the NSA paid or not? Is confidentiality still preserved? Briefly explain why or why not.

Answer:

$\top$ (truth) to model "different", heads
$\bot$ (falsity) to model "equal", tails

Claim:

$a1 \oplus a2 \oplus a3 = \top$ iff there's an odd number of diffs
$a1 \oplus a2 \oplus a3 = \bot$ iff there's an even number of diffs

Case 1: Suppose NSA paid

$$
\begin{aligned}
& a1 \oplus a2 \oplus a3 \\
&= \neg(t1 \oplus t3) \oplus \neg(t2 \oplus t1) \oplus \neg(t3 \oplus t1) \\
&= \neg t1 \oplus t3 \oplus \neg t2 \oplus t1 \oplus \neg t3 \oplus t1 \\
&= (\neg t1 \oplus t1) \oplus (\neg t2 \oplus t2) \oplus (\neg t3 \oplus t3) \\
&= \top \oplus \top \oplus \top \\
&= \top
\end{aligned}
$$

Case 2: Suppose one of us paid (C1 paid)

$$
\begin{aligned}
& a1 \oplus a2 \oplus a3 \\
&= t1 \oplus t3 \oplus \neg(t2 \oplus t1) \oplus \neg(t3 \oplus t1) \\
&= t1 \oplus t3 \oplus \neg t2 \oplus t1 \oplus \neg t3 \oplus t1 \\
&= (t1 \oplus t1) \oplus (\neg t2 \oplus t2) \oplus (\neg t3 \oplus t3) \\
&= \bot \oplus \top \oplus \top \\
&= \bot
\end{aligned}
$$

Therefore:

It can prove that an odd number of "diff." means the NSA paid. An even number of "diff." means one of the C_i paid.

Safety and Liveness (5 marks)

Limit closures

Let s be a state, and let s^ω denote the behaviour $ssssssssssss$ ... (i.e. infinitely many repetitions of s.)

Give an example of a set A such that $s^\omega \in \bar{A}$, but $s^\omega \notin A$.

Answer:

When set A is a liveness property and no finite prefix of s ever fulfills the promise of the liveness property.

Alpern and Schneider's theorem

1. Let $\Sigma = \{a, b\}$. That is, we assume there are only two states, a and b. Consider the property $P = \{\sigma | \sigma \; contains \; exactly \; one \; b\}$. Use Alpern and Schneider's theorem to decompose P into a safety property P_S and a liveness property P_L. Simplify them; that is, don't just say $P_L = \Sigma^\omega \setminus (\bar{P} \setminus P)$ but give something that explains what P_L is.
2. Assume P is a safety property. Prove that $\Sigma^\omega \setminus (\bar{P} \setminus P) = \Sigma^\omega$ using the algebraic laws of set operations.
3. Is the empty property $\emptyset$ a liveness property? Is it a safety property? Explain.

Answer:

1. $P = \bar{P} \cap \Sigma^\omega \setminus (\bar{P} \setminus P)$

2.

3. $\emptyset = \Sigma^\omega \cap \Sigma^+$, $liveness \; properties \; are \; not \; closed \; under \; finite \; intersection, \emptyset \; is \; not \; liveness$ property.

Temporal Logic (5 marks)

Examples

Define suitable predicate symbols and give LTL formalisations for the following properties:

1. Once the dragon was slain, the princess lived happily ever after.
2. The dragon was never slain, but the princess lived happily until she didn't.
3. The dragon was slain at least twice.
4. The dragon was slain at most once.
5. Whenever the dragon was slain, the princess did not live happily.

Answer:

Define φ *The dragon be slain*

Define ψ *the princess live happily*

Define $\sigma = \sigma_0\ \sigma_1\ \sigma_2\ \sigma_3\ \sigma_4$ *be a behavior of kill dragon or not kill dragon*

1. *Before kill the fragon*: $\varphi\ \mathcal{U}\ \psi$

   After *kill the fragon*: $\Box\psi$

2. $\Box\neg\varphi, \psi\ \mathcal{U}\neg\psi$

3. $\sigma \vDash \varphi,\ \ \sigma \vDash \bigcirc\varphi,\ \sigma|_2 \vDash \Diamond\varphi$

4. $\sigma \vDash \bigcirc\Box\neg\varphi$

5. $\sigma \vDash (\neg\varphi \wedge \psi)\ \mathcal{U}\ (\varphi \wedge \neg\psi)$

Proof

Prove the following logical statements:

$$\Box\Box\varphi \Leftrightarrow \Box\varphi$$

$$\Diamond\bigcirc\varphi \Leftrightarrow \bigcirc\Diamond\varphi$$

$$\Box\varphi \Leftrightarrow \Diamond\varphi$$

It may help to use these semantic definitions for $\Box$ and $\Diamond$ (derivable from the definition in terms of $\mathcal{U}$):

$$\sigma \vDash \Diamond\varphi \quad iff \quad \exists_i \geq 0.\ (\sigma|_i \vDash \varphi)$$

$$\sigma \vDash \Box\varphi \quad iff \quad \exists_i \geq 0.\ (\sigma|_i \vDash \varphi)$$

You may use previously proven identities (both in this question and in lectures) to prove new ones.

Note that two temporal logic formulas ϕ and ψ are logically equivalent, written $\varphi \Leftrightarrow \psi$, iff for all behaviours σ it holds that:

$$\sigma \vDash \varphi \text{ if and only if } \sigma \vDash \psi$$

Answer:

$\Box\Box\, \varphi \Leftrightarrow \Box\, \varphi$

$Proof$:

$\Diamond \bigcirc \varphi \Leftrightarrow \bigcirc \Diamond \varphi$

$Proof$:

$\sigma \vDash \bigcirc \Diamond \varphi$

Iff (by def)

$\sigma|_1 \vDash \Diamond \varphi$

Iff (by def)

$\exists_i \geq 0.\ (\sigma|_{i+1} \vDash \varphi)$

Iff (by def)

$\exists_i \geq 0.\ (\sigma|_i \vDash \bigcirc \varphi)$

Iff (by def)

$\sigma \vDash \Diamond \bigcirc \varphi$

$\Box\, \varphi \Leftrightarrow \Diamond\, \varphi$

$Proof$:

$\sigma \vDash \Diamond\, \varphi$

Iff (by def)

$\exists_i \geq 0.\ (\sigma|_i \vDash \varphi)$

Iff (by def)

$\sigma \vDash \Box\, \varphi$