Homework Week 1

Circularity

What is the answer to this question?

Leslie Lamport's pants

Dining Cryptographers

paying cryptographers now tell the truth about whether the coin tosses are different or equal, vice versa.

There are two possible cases:

1. **Two of them lied – one of them paid.**
2. **They all lied – NSA paid.**

This protocol is equivalent to the original one, and it can be proven in two ways: one is to induce that this protocol works based on the proposition that the original works, and the other is to enumerate cases.

If we assume that the original protocol works, we can have these two cases:

1. **Two of them told a truth – one of them paid.**
2. **They all told truth – NSA paid.**

If they do one more step, that is, take the negation of the claim in mind, each truth would become a lie. The cases would be:

1. **Two of them told a lie – one of them paid.**
2. **They all told lies – NSA paid.**

which is exactly the same as the new protocol.

To deduce logically we can define:

t_i as the result of coin tossed by ith crytographer. a_i as the claim made by ith crytographer given no lie.

Then we have:

$$r_1 = \neg a_1 \oplus \neg a_2 \oplus a_3 = \neg t_1 \oplus t_3 \oplus \neg t_2 \oplus t_1 \oplus t_3 \oplus t_2 = \top \oplus \top \oplus \bot = \bot$$

In case 1. And there is also:

$$r_2 = \neg a_1 \oplus \neg a_2 \oplus \neg a_3 = \neg t_1 \oplus t_3 \oplus \neg t_2 \oplus t_1 \oplus \neg t_3 \oplus t_2 = \top \oplus \top \oplus \top = \top$$

In case 2.

Therefore, we can always determine whether NSA paid the bill by the taking $\oplus$ of all the claims. If the result is true, we can say the NSA paid.

Safety and Liveness

Limit closures

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

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

Define A as a set of behaviour that for any natural number n, there is always a behaviour whose first n states are s and followed by at least one other non-s state.

Example:

$$A = \{so,$$
$$sso,$$
$$ssso,$$
$$sssso,$$
$$ss \dots sso \dots\}$$

Thus, for any behaviour in A that have common n first common states, there always exists a natural number p that a non-s state occurs in first $n + p$ states. And obviously, $s^\omega \in \bar{A}$. Therefore, we have $s^\omega \in \bar{A}$ but $s^\omega \notin A$.

Alpern and Schneider's theorem

1. ***Decompose*** $\boldsymbol{P = \{\sigma | \sigma \text{ contains exactly one } b\}}$ ***into*** $\boldsymbol{P_S}$ ***and*** $\boldsymbol{P_L}$***.***

$$P_S = \{\sigma | \sigma \text{ contains at most one } b\}$$

$$P_L = \{\sigma | \sigma \text{ contains at least one } b\}$$

2. ***Assume P is a safety property. Prove that*** $\boldsymbol{\Sigma^\omega \backslash (\bar{P} \backslash P) = \Sigma^\omega}$ ***using the algebraic laws of set operations.***

Because a safety property is limit closed, according to the question, we have:

$$P = \bar{P}.$$

Then, the expression can be transformed as follows:

$$\begin{aligned} &\Sigma^\omega \backslash (\bar{P} \backslash P) \\ &= \Sigma^\omega \backslash (\bar{P} \backslash \bar{P}) \\ &= \Sigma^\omega (\bar{P} \cap P^c) \\ &= \Sigma^\omega \backslash \emptyset \ (complement\ law) \\ &= \Sigma^\omega \cap \Sigma^\omega \\ &= \Sigma^\omega \ (idempotent\ law) \end{aligned}$$

3. ***Is the empty property*** $\emptyset$ ***a liveness property? Is it a safety property? Explain.***

It is **not a liveness** property, because no behaviour is in the set, which means that nothing desired would happen.

It is a **safety** property, because no behaviour is in the set, which means that no violation would happen. In addition, $\overline{\emptyset} = \emptyset$ means that empty property is limit closed, which is a feature of safety property.

Temporal Logic

Examples

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

Define dragon slain as s and princess lives happily as h. The world is represented by a behaviour σ consisting of s and h in this question.

1. ***Once the dragon was slain, the princess lived happily ever after.***

The LTL formalisation is: $\sigma \vDash \diamond (s \wedge \circ \Box h) \wedge \neg \diamond (s \wedge \circ\diamond \neg h)$

2. The dragon was never slain, but the princess lived happily until she didn't.

The LTL formalisation is: $\sigma \vDash (\neg \diamond s) \wedge (h \,\mathcal{U}\, \neg h)$

3. The dragon was slain at least twice.

The LTL formalisation is: $\sigma \vDash \diamond (s \wedge \circ\diamond s)$

4. The dragon was slain at most once.

The LTL formalisation is: $\sigma \vDash (s \wedge \circ \Box\neg s) \vee \left(\neg s \mathcal{U} (s \wedge \circ \Box\neg s)\right)$

5. Whenever the dragon was slain, the princess did not live happily.

The LTL formalisation is: $\sigma \vDash \neg \diamond (s \wedge h)$

Proof

1

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

By definition,

$$\sigma \vDash \Box\varphi \; iff \;\; \forall i \geq 0. (\sigma|_i \vDash \varphi)$$

Thus, we have:

$$\sigma \vDash \Box\Box\varphi \; iff \;\; \forall i \geq 0. (\sigma|_i \vDash \Box\varphi)$$

$$\Leftrightarrow \forall i \geq 0, \forall j \geq i. \left(\sigma|_{i+j} \vDash \varphi\right)$$

The above statement can be simplified as:

$$\sigma \vDash \Box\Box\varphi \; iff \;\; \forall k \geq 0. (\sigma|_k \vDash \varphi)$$

Which is the same as the definition of $\sigma \vDash \Box\varphi$.

2

$$\diamond\circ \varphi \Leftrightarrow \circ\diamond \varphi$$

$\diamond\circ \varphi$ can be defined as:

$$\sigma \vDash \diamond\circ \varphi \; iff \; \exists i \geq 0. (\sigma|_i \vDash \circ \varphi)$$

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

$\circ\diamond\varphi$ can be defined as:

$$\sigma \vDash \circ\diamond\varphi \; iff (\sigma|_1 \vDash \diamond\varphi)$$

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

Which is exactly the same the definition of $\diamond\circ\varphi$.

3

$$\Box\varphi \Longrightarrow \diamond\varphi$$

The definition of $\Box\varphi$ is:

$$\sigma \vDash \Box\varphi \; iff \; \forall i \geq 0. (\sigma|_i \vDash \varphi)$$

Then $\neg\Box\varphi$ is:

$$\sigma \vDash \neg\Box\varphi \; iff \; \exists i \geq 0. (\sigma|_i \vDash \neg\varphi)$$

And the definition of $\diamond\varphi$ is:

$$\sigma \vDash \diamond\varphi \; iff \; \exists i \geq 0. (\sigma|_i \vDash \varphi)$$

Hence, $\Box\varphi \Longrightarrow \diamond\varphi$ can be written as:

$$\neg\Box\varphi \vee \diamond\varphi$$
$$\Leftrightarrow \neg\Box\varphi \vee \neg\Box\neg\varphi$$
$$\Leftrightarrow \top$$