HW1 - Dan Nguyen (z5206032)

Circularity

Leslie Lamport's pants

Dining Cryptographers

Consider the dining cryptographers problem where the cryptographers, C_1, C_2, C_3, tell the truth about whether the coin tosses are different or equal and will lie about whether they got heads or tails.

To determine if their dinner was paid for anonymously by either one of the three cryptographers or the NSA:

- Each C_i tosses a coin, t_i.
- Each C_i tells what they tossed only to their right and will lie about their toss only if they paid.
- Each C_i truthfully makes an announcement, a_i, if the two coin tosses are equal or different.

Do we still know if the NSA paid or not? Is confidentiality still preserved?

Test:

$$\top \oplus \top = \bot$$
$$\top \oplus \bot = \top$$

Define announcements a_i in terms of tosses:

$$a_1 \oplus a_2 \oplus a_3 = (t_1 \oplus t_2) \oplus (t_2 \oplus t_3) \oplus (t_3 \oplus t_1)$$

If the NSA paid then each cryptographer tells the truth about their toss:

$$\begin{aligned} a_1 \oplus a_2 \oplus a_3 &= (t_1 \oplus t_2) \oplus (t_2 \oplus t_3) \oplus (t_3 \oplus t_1) \\ &= (\top \oplus \top) \oplus (\top \oplus \top) \oplus (\top \oplus \top) \\ &= \bot \oplus \bot \oplus \bot \\ &= \bot \end{aligned}$$

If one of the cryptographers paid then that cryptographer lies about their toss (let this cryptographer be C_1):

$$\begin{aligned} a_1 \oplus a_2 \oplus a_3 &= (t_1 \oplus t_2) \oplus (t_2 \oplus t_3) \oplus (t_3 \oplus t_1) \\ &= (\bot \oplus \top) \oplus (\top \oplus \top) \oplus (\top \oplus \bot) \\ &= \top \oplus \bot \oplus \top \\ &= \bot \end{aligned}$$

It is clear to see that despite one of the cryptographers lying about their coin toss, we cannot determine if the NSA has paid or not.

Confidentiality is still preserved.

Safety and Liveness

Limit Closures

Let s be a state.

Let s^ω denote the behaviour $sssss\ldots$ i.e. infinitely many reptitions of s.

An example of a set A s.t. $s^\omega \in \overline{A}$ but $s^\omega \notin A$ is:

$$\overline{A} = \{s, ss, sss, \ldots\}$$
$$A = s$$

Alpern and Schneider's Theorem

Part 1

Let $\Sigma = \{a, b\}$.

Consider the property:

$$P = \{\sigma | \sigma \text{ contains exactly one } b\}$$
$$= \{ \overbrace{a, \ldots, a}^{0 \text{ to } \backslash\text{infin times}}, b\}$$

Let:

- P_S be the decomposed safety property of P.
- P_L be the decomposed liveness property of P.

Alpern and Schneider's Theorem states:

$$P = \overbrace{\overline{P}}^{\text{closed}} \cap \overbrace{\Sigma^\omega \setminus (\overline{P} \setminus P)}^{\text{dense}}$$

The safety property of P is simply:

$$P_S = \overline{P}$$
$$= \{ \overbrace{a, \ldots, a}^{0 \text{ to } \backslash\text{infin times}}, b\}$$

The liveness property of P is:

$$\begin{aligned} P_L &= \Sigma^\omega \setminus (\overline{P} \setminus P) \\ &= \Sigma^\omega \setminus (\overline{P} \cap P^c) \\ &= \Sigma^\omega \cap (\overline{P} \cap P^c)^c \\ &= \Sigma^\omega \cap (\overline{P}^c \cup P) \\ &= \Sigma^\omega \cap (P_S^c \cup P) \\ &= \Sigma^\omega \cap (\{ \overbrace{a, \ldots, a}^{0 \text{ to } \backslash\text{infin times}}, b\}^c \cup \{ \overbrace{a, \ldots, a}^{0 \text{ to } \backslash\text{infin times}}, b\}) \end{aligned}$$

To explain P_L, eventually within the universe, we will get a set that contains exactly one b for any number of a; or we will get a set that

does not have exactly one b for any number of a.

Part 2

Assume P is a safety property, so:

$$P = \overline{P}$$

Consider the dense set of P:

$$\begin{aligned}\Sigma^\omega \setminus (\overline{P} \setminus P) &= \Sigma^\omega \setminus (\overline{P} \cap P^c) \\ &= \Sigma^\omega \cap (\overline{P} \cap P^c)^c \\ &= \Sigma^\omega \cap (\overline{P}^c \cup P) \\ &= \Sigma^\omega \cap (P^c \cup P) \\ &= \Sigma^\omega \cap (\Sigma^\omega) \\ &= \Sigma^\omega \text{ as required}\end{aligned}$$

Part 3

Consider the limit closure of $\emptyset$:

$$\overline{\emptyset} = \emptyset \therefore \emptyset \text{ is a safety property}$$

We can assume that $\emptyset$ is a safety property, so using the result from part 2, we consider the denseness of $\emptyset$:

$$\begin{aligned}\Sigma^\omega \setminus (\overline{\emptyset} \setminus \emptyset) &= \Sigma^\omega \setminus (\overline{\emptyset} \cap \emptyset^c) \\ &= \Sigma^\omega \\ &\neq \emptyset \therefore \emptyset \text{ is not a liveness property}\end{aligned}$$

Temporal Logic

Examples

Let:

- D be state where dragon is alive; otherwise $\neg D$.
- P be state where princess lives happily ever after; otherwise $\neg P$.

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

$$\sigma \models (D \wedge \neg P)\, \mathcal{U}\, (\neg D \wedge P)$$

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

$$\sigma \models (\Box \neg D) \wedge (P\, \mathcal{U}\, \neg P)$$

3. The dragon was slain at least twice.

$$\sigma \models \Diamond \neg D \wedge \bigcirc (\Box \Diamond \neg D)$$

“

Eventually the dragon is slain, and after this the dragon is always eventually slain.

4. The dragon was slain at most once.

$$\sigma \models \Diamond \neg D \wedge \bigcirc(\Box D)$$

“

Eventually the dragon is slain, and after the dragon is always not slain.

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

$$\sigma \models (D \wedge P) \vee (D \wedge \neg P) \vee (\neg D \wedge \neg P)$$

Proof

Part 1

Prove:

$$\Box\Box\phi \iff \Box\phi$$

Let:

$$\sigma \models \Box\phi$$

Proof:

$$\begin{aligned}\sigma \models \Box\phi &= \forall i.\ \sigma|_i \models \phi \\ &= \forall \sigma.\ \sigma \models (\forall i.\ \sigma|_i \models \phi) \\ &= \sigma \models \Box(\forall i.\ \sigma|_i \models \phi) \\ &= \sigma \models \Box\Box\phi \text{ as required}\end{aligned}$$

Part 2

Prove:

$$\Diamond \bigcirc \phi \iff \bigcirc\Diamond\phi$$

Let:

$$\sigma \models \Diamond \bigcirc \phi$$

Proof:

$$\begin{aligned}\sigma \models \Diamond \bigcirc \phi &= \sigma \models \Diamond(\bigcirc \phi) \\ &= \exists i + 1.\ \sigma|_{i+1} \models \phi \\ &= \sigma \models \bigcirc(\exists i.\ \sigma|_i \models \phi) \\ &= \sigma \models \bigcirc\Diamond\phi \text{ as required}\end{aligned}$$

Part 3

Prove:

$$\Box\phi \implies \Diamond\phi$$

Let:

$$\sigma \models \Box\phi$$

Proof:

$$\begin{aligned}\sigma \models \Box\phi &= \forall i.\ \sigma|_i \models \phi \\ &= \exists i.\ \sigma|_i \models \phi \\ &= \sigma \models \Diamond\phi \text{ as required}\end{aligned}$$

> *Note that this proof does not imply the reverse since* $\exists\sigma|_i$ *does not mean* $\forall\sigma|_i$.