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:*

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

Then we have:

In case 1. And there is also:

In case 2.

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

# Safety and Liveness

## Limit closures

***Let  be a state, and let  denote the behaviour ssssssssssss…ssssssssssss… (i.e. infinitely many repetitions of ss.)***

***Give an example of a set A such that , but .***

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

Example:

Thus, for any behaviour in that have common first common states, there always exists a natural number that a non- state occurs in first states. And obviously, . Therefore, we have but .

## Alpern and Schneider's theorem

1. ***Decompose into and .***
2. ***Assume P is a safety property. Prove that using the algebraic laws of set operations.***

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

Then, the expression can be transformed as follows:

1. ***Is the empty property 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, 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 and princess lives happily as . The world is represented by a behaviour consisting of and in this question.

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

The LTL formalisation is:

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

The LTL formalisation is:

1. ***The dragon was slain at least twice.***

The LTL formalisation is:

1. ***The dragon was slain at most once.***

The LTL formalisation is:

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

The LTL formalisation is:

## Proof

### 1

By definition,

Thus, we have:

The above statement can be simplified as:

Which is the same as the definition of .

### 2

can be defined as:

can be defined as:

Which is exactly the same the definition of .

### 3

The definition of is:

Then is:

And the definition of is:

Hence, can be written as: