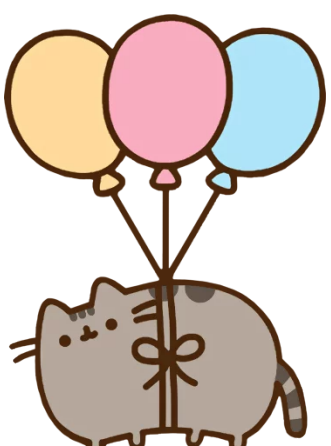
开题报告 - 使用定理证明系统验证路由协议

计算机网络中的形式化方法与协议工程学

刘晓义 罗云千



TL;DR

TL;DR

- 内嵌 LTL 模态逻辑到 Coq 中，定义路由协议 Specification
  - $\vdash \Box P$
-

TL;DR

- 内嵌 LTL 模态逻辑到 Coq 中，定义路由协议 Specification
  - $\vdash \Box P$
- 使用 Coq 给出一个实现，附带 Invariants，自动合成其余正确性的证明。

Constructing the specification

“消息传递模型”： 每个 Frame（时间点）对应一个传输事件：输入消息或者输出消息。

Constructing the specification

“消息传递模型”： 每个 Frame（时间点）对应一个传输事件：输入消息或者输出消息。

- 消息结构通过归纳数据类型定义
- 引入一元谓词: $I(m), O(m)$: 输入输出路由消息
- 引入二元谓词: $R(a, n)$: 路由表

Constructing the specification

“消息传递模型”： 每个 Frame（时间点）对应一个传输事件：输入消息或者输出消息。

- 消息结构通过归纳数据类型定义
- 引入一元谓词: $I(m), O(m)$: 输入输出路由消息
- 引入二元谓词: $R(a, n)$: 路由表

$$I(...) \rightarrow R(...)UI(...)$$

Embedding

为上述谓词添加一个“时刻”:

$$I(...) \rightarrow R(...)UI(...)$$

Embedding

为上述谓词添加一个“时刻”:

$$I(...) \rightarrow R(...)UI(...)$$

$$\forall t_1, (I(t_1, i) \rightarrow$$

$$\forall t_2 > t_1, (\forall t_3 \in (t_1, t_2), \neg I(t_3, ...)) \rightarrow R(t_2, ...))$$

Embedding

为上述谓词添加一个“时刻”:

$$I(...) \to R(...)UI(...)$$

$$\forall t_1, (I(t_1, i) \to$$

$$\forall t_2 > t_1, (\forall t_3 \in (t_1, t_2), \neg I(t_3, ...)) \to R(t_2, ...))$$

- LTL Worlds $\sim\mathbb{N} \rightsquigarrow t \in \mathbb{N}$
- 这一任务可以自动化进行

Conformance proof: The easier part

Wire-format ⇔ 消息表示:

Conformance proof: The easier part

Wire-format ⇔ 消息表示:

问题：Illegal packets

Conformance proof: The easier part

Wire-format ⇔ 消息表示:

问题：Illegal packets

Failable parser & handler: 给定 $t, m, \neg I(t, m)$ 可判定。

```
Definition Parser : Set := Frame -> Result Message Error
Definition Handler : Set :=
  State -> Message -> State × Option Error
```

Conformance proof: The harder part

状态机和路由表的性质

Conformance proof: The harder part

状态机和路由表的性质

Invariant 手动给出，其他部分的 Weakest-precondition 是可判定的。

Coq: `firstorder`: 尝试证明 $\mathrm{WP} \to P$

Expected things

- 一个 Formal semantics
- 一个正确的实现
- (Optionally) 部分并行系统性质的证明 (e.g. 收敛性，正确性等)

Alternatives

LTL 自己存在一个证明系统，但是并不存在配套的定理证明工具。

Thank you!