Hoare soundness proof

Claim Soundness for partial correctness. if $\vdash \{p\}c\{q\}$, then $\models \{p\}c\{q\}$.

Definition 0.1. $\models \{p\}c\{q\}$

$\models \{p\}c\{q\} \iff \forall\sigma,\sigma'.(\sigma \models p) \wedge ((c,\sigma) \longrightarrow^* (skip,\sigma')) \Rightarrow (\sigma' \models q)$

Definition 0.2. $\vdash \{p\}c\{q\}$

There exists a proof or derivation for $\{p\}c\{q\}$.

用自然语言描述，我们要证明满足 p 的所有状态 σ，在执行语句 c 后（按照语义定义进行 evaluate），或者不终止，或者终态满足 q.

首先我们希望描述对某单一初始状态 σ，相对于语句 c 和终态 q 的“soundness”，也就是课件中定义的 $Safe(c,\sigma,q)$. 这一步可以理解为设立一个中间目标替换 $\models \{p\}c\{q\}$，去掉 σ 前的全称量词，以进行 inductive 的证明。如果对于某个 p，所有符合它的状态都满足这种描述，那么就是符合语义的了。

Definition 0.3. $Safe^n(c,\sigma,q)$

$Safe^0(c,\sigma,q)$ always holds;

$Safe^{n+1}(c,\sigma,q)$ holds iff (a) c = skip and $\sigma \models q$; or (b) there exists c' and σ' such that $(c,\sigma) \longrightarrow (c',\sigma')$ and $Safe^n(c',\sigma',q)$.

We say $Safe(c,\sigma,q)$ iff $Safe^n(c,\sigma,q)$ holds for all n.

用自然语言描述：某一个状态 σ 对于某指令 c 和某谓词 q 是 Safe 的，当它存在某一条不终止的执行方式，或者一条终止的、且终态满足 q 的执行方式。（即允许歧义性）

Lemma 1. $Safe(c,\sigma,q) \Rightarrow ((c,\sigma) \longrightarrow^* (skip,\sigma')) \Rightarrow (\sigma' \models q)$

证明. 我们对 Safe 的定义是直接为 Lemma1 服务的，它的证明也应是 obvious 的. Follow by lemma 1.1 and lemma 1.2. 但我认为 lemma1.2 不是 trival 的 (要求没有二义性就好了). □

Lemma 1.1 Progress. If $Safe(c, \sigma, q)$, then either c is skip, or there exists c' and σ' such that $(c, \sigma) \longrightarrow (c', \sigma')$.

证明. Trival. □

Lemma 1.2 Preservation. If $Safe(c, \sigma, q)$ and $(c, \sigma) \longrightarrow (c', \sigma')$, then $Safe(c', \sigma', q)$.

证明. 并不能看出这一步是 trival 的，因为它要求语义是没有二义性的。 □

Lemma 2. $\vdash \{p\}c\{q\} \Rightarrow \forall\sigma.(\sigma \models p) \Rightarrow Safe(c, \sigma, q)$

证明. Proof by induction over the derivation of $\vdash \{p\}c\{q\}$. □

Lemma 3. Lead to Soundness. $lemma1 \wedge lemma2 \Rightarrow \vdash \{p\}c\{q\} \Rightarrow (\forall\sigma, \sigma'.((\sigma \models p) \wedge ((c, \sigma) \longrightarrow^* (skip, \sigma'))) \Rightarrow (\sigma' \models q))$

证明. Trival. □