1999

p8q2
MJCG

Specification & Verification 1: Solution Notes to Question 2

```
|- {T} SKIP {T}                          SKIP-axiom
|- {T /\ T} SKIP {T}                     Precondition strengthening
|- {T} WHILE T DO SKIP {T /\ ~T}         WHILE-rule
```

WHILE T DO SKIP never terminates so [T] WHILE T DO SKIP [T /\ ~T] is false, hence by soundness of Hoare logic for total correctness it is not the case that |- [T] WHILE T DO SKIP [T /\ ~T].

```
{X=x /\ Y=y} TEMP := X; X := Y; Y := TEMP {X=y /\ Y=x}
```

Is translated to:

```
 Spec((\s. s`X`=x /\ s`Y`=y),
      Seq(Assign(`TEMP`,\s. s`X`),
          Seq(Assign(`X`,\s. s`Y`),Assign(`Y`,\s. s`TEMP`))),
      (\s. s`X`=y /\ s`Y`=x))
```

where

```
   Spec(p,c,q) = !s1 s2. p s1 /\ c(s1,s2) ==> q(s2)

   Seq(c1,c2)(s1,s2) = ?x. c1(s1,s) /\ c2(s,s2)

   Assign(v,e)(s1,s2) = (s2 = \x. (x=v => e s | s x))
```

The following is correctly annotated:

```
   {T} WHILE T DO{F} SKIP {F}
```

As shown above (plus T /\ ~T ==> F) it is the case that:

```
   |- {T} WHILE T DO SKIP {F}
```

but the VCs are:

1. T ==> F
2. F /\ ~T ==> F
3. ~T /\ F ==> F

clearly 1 is false (2 and 3 are true).

The significance is that truth of VCs is a sufficient, but not necessary, condition for the original specification to be proveable.

[P,Q] is the set of commands C such that |- [P]C[Q] (i.e. {C | |- [P]C[Q]})

WHILE-law is:

$$\frac{\vdash P \wedge S \Longrightarrow E \geq 0}{[P,\ P \wedge \neg S] \gg \text{WHILE } S \text{ DO } [P \wedge S \wedge E{=}n,\ P \wedge E{<}n]}$$

Derivation:

```
C in WHILE S DO [P /\ S /\ E=n, P /\ E<n]
<==> C in {WHILE S DO C' | C' in [P /\ S /\ E=n, P /\ E<n]}
<==> C in {WHILE S DO C' | |- [P /\ S /\ E=n] C' [P /\ E<n]}
<==> C in {WHILE S DO C' | |- [P] WHILE S DO C' [P /\ ~S]}
 ==> |- [P] C [P /\ ~S]
<==> C in [P, P /\ ~S]
```