Problem 5.12 $pal_2(S)$

$X \leftarrow S$

$E \leftarrow T$

// $isPal(S) \Leftrightarrow E = T \wedge isPal(X)$

while $(X \neq \Lambda) \wedge E = T$.

if $eq(head(X), tail(X))$

$X \leftarrow all\text{-}but\text{-}last(tail(X))$

else $E \leftarrow \perp$.

return E.

// Q: $isPal(S) \Leftrightarrow E = T$.

(a) Pal_2 is partially correct? (YES)

(2) Termination? (NO).

5.10. ~~reverse~~ Pal1(S)

```
Y ← rev(S)
return Equal(S, Y)
```

⇒

```
pal1(S)
//(0) P: T.
Y ← rev(S)
// (1) Y = reverse(S)
E ← Equal(S, Y)
return E
```

// Q: isPal(S) ⇔ E = T.

pf. (1) Partial correctness.

(1) { E ← equal(S, Y) } Q.

Y = reverse(S) ∧ E = equal(S, Y)

⇒ E = equal(S, reverse(S))

By def of Pal ⇒ E = T ⇔ isPal(S).

pf. (2) Termination.

5.6 reverse(S).

(a) Structure of reverse. (3 invariants).

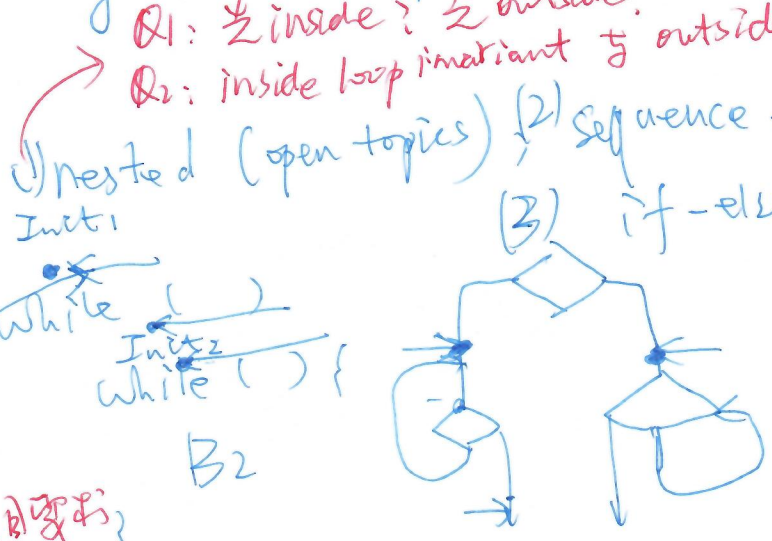
(b) only "start" + "stop",

(c) Q1: 关 inside ? 关 outside?

Q2: inside loop invariant 与 outside loop invariant 是什么关系?

(d) (1) Nested (open topics) (2) Sequence.

(3) if-else.



Euclid Alg.

```
Euclid (m, n):
    if n = 0
        return m
    else
        return Euclid(n, m%n)
```

- Input: nonnegative integer m, n

Def: gcd(0,0) = 0

gcd(a,0) = a.

Termination: $m \% n < n$

Note: if $0 \le m < n$

↳ Euclid(n, m)

Thm. $\gcd(m,n) = \gcd(n, m \bmod n)$.

Pf. $\gcd(m,n) = d$

$\gcd(m, m \bmod n) = d'$

(1) $d \mid d'$ (2) $d' \mid d$.

(1) $d \mid d'$.

$d = \gcd(m,n)$

$d \mid m$

$d \mid n$

$\Rightarrow d \mid n$

$d \mid (m \bmod n)$

$= m - nq$

$q = \lfloor m/n \rfloor$

(2) $d' \mid d$

$d' = \gcd(n, m\%n)$

$d' \mid n$

$d' \mid (m \bmod n)$

$m = qn + m \bmod n$

$\Rightarrow d' \mid m$

$\Rightarrow d' \mid \gcd(m,n)$

$d' \mid d$.

Partial correctness:

Thm: $\gcd(m,n) = \gcd(n, m \bmod n)$. 且 $\gcd(m,0) = m$

$= \dots$

$= \gcd(m', 0)$ (Def) $= m'$

(alg.) m'.

Pf by mathematical induction on n (m,n).

注意这与 gcd 与 Euclid(m,n) 与 alg 的对应.

Basis: $n = 0$. $\gcd(m,n) = \gcd(m,0) =$ Euclid(m,n).

I.H. $\gcd(m,k) =$ Euclid(m,k). $k \le n-1$

I.S. to prove $\gcd(m,n) =$ Euclid(m,n) $n \ge 1$

Euclid(m,n) = Euclid(n, m mod n)

$m \bmod n < n$

$= \gcd(n, m \bmod n)$.

By I.H. $\gcd(m,n) = \gcd(n, m \bmod n)$.