1999

p7q2

MJCG

Specification & Verification 1: Solution Notes to Question 1

The first part is bookwork. The main point is that an array assignment

```
A(n) := E
```

should be treated as an ordinary assignment to a function:

```
A := A{n <- E}
```

2 marks for this. Another 2 marks for mentioning that reasoning about arrays often uses the following laws for function updates:

```
A{n <- E}(n) = E

A{n <- E}(m) = A(m)    if m is not equal to n
```

The properties:

```
!n. 0<=n ==> Sigma2(A,n,n) = A(n)
```

and

```
!m n.
 0<=m /\ m<n
 ==> Sigma2(A,m,n) = A(m) + A(n) + Sigma2(A,m+1,n-1)
```

each follows by just expanding definitions and then doing case analysis and arithmetical cancelling. Give 1 mark for the first one, 2 for the second and an additional mark for good presentation (so 4 in total)

For the Floyd-Hoare proof, the loop can then be verified using the invariant:

```
Sigma(A,n) = SUM + Sigma2(A,M,N) /\ 0<=M
```

This clearly holds after M := 0; SUM := 0, assuming initially N=n.

To verify invariance there are two cases:

Case M=N. Need to show:

```
N<=N /\ Sigma(A,n) = SUM + Sigma2(A,N,N) /\ 0<=N
==>
Sigma(A,n) = SUM + A(N) + Sigma2(A,N+1,N) /\ 0<=N+1
```

This follows directly from the definitions and the first property.

Case M<N. Need to show:

```
M<=N /\ Sigma(A,n) = SUM + Sigma2(A,M,N) /\ 0<=M
==>
Sigma(A,n) = SUM + A(M) + A(N) + Sigma2(A,M+1,N-1) /\ 0<=M+1
```

Assuming 0<=M and M<N, by the second property:

```
SUM + Sigma2(A,M,N)  =  SUM + A(M) + A(N) + Sigma2(A,M+1,N-1)
```

Thus the invariant works in this case also.

On termination:

```
~(M<=N) /\ Sigma(A,n) = SUM + Sigma2(A,M,N) /\ 0<=M /\ 0<=N
==>
N<M /\ Sigma(A,n) = SUM + Sigma2(A,M,N)  ==> Sigma(A,n) = SUM
```

Give roughly 6 marks for inventing and verifying the invariant; 4 marks for the other parts of the proof, including the initialisation and case split; 2 marks for good presentation.
Thus 12 marks in total for the Floyd-Hoare proof.