Chương 4

KIỂM TRA TÍNH ĐÚNG CỦA MODULE

4.1. Khái niệm chung

Như đã nói ở trước, sản phẩm phần mềm được gọi là đúng nếu nó thực hiện được chính xác những tiêu chuẩn mà người thiết kế đã đặt ra. Để có một đánh giá chính xác về cấp độ đúng của phần mềm, ta phải kiểm tra chất lượng phần mềm. Như thế, kiểm tra là quá trình tìm lỗi và nó là một đánh giá cuối cùng về các đặc tả, thiết kế và mã hoá. Mục đích của kiểm tra là đảm bảo rằng tất cả các thành phần của ứng dụng ăn khớp, vận hành như mong đợi và phù hợp các tiêu chuẩn thiết kế. Một phương pháp theo cách tiếp cận giảm thiểu sót về 0 là áp dụng suy diễn toán học cho đòi hỏi logic, chứng minh tính đúng đắn của chương trình. Phương pháp này đòi hỏi đặc tả ngôn ngữ dạng hình thức để có thể chứng minh tính đúng đắn của chương trình thông qua các dòng lệnh đã viết.

Như ta đã biết, chương trình P là một bộ biến đổi tuần tự P để chuyển cái vào x thành ra cái y; ở đây x và y hoàn toàn được xác định trước.

Như vậy, một chương trình P được gọi là đúng nếu nó thực hiện chính xác những mục tiêu do người thiết kế đặc ra. Ta gọi:

+ Giả thiết $\{A\}$ là mệnh đề được phát biểu để thể hiện tính chất của cái vào, gọi tắt là mệnh đề dữ liệu vào.

+ Kết luận $\{B\}$ là mệnh đề được phát biểu để tính chất cần có của dữ liệu ra, gọi tắt là mệnh đề dữ liệu ra.

Do P có tính tuần tự và hữu hạn nên có thể biểu diễn P là một dãy liên tiếp các cấu trúc điều khiển P_1, P_2,....,P_n. Do vậy, bằng cách nào đó mà ta khẳng định được:

P_1 biến đổi $\{A\}$ thành $\{A_1\}$

P_2 biến đổi $\{A_1\}$ thành $\{A2\}$

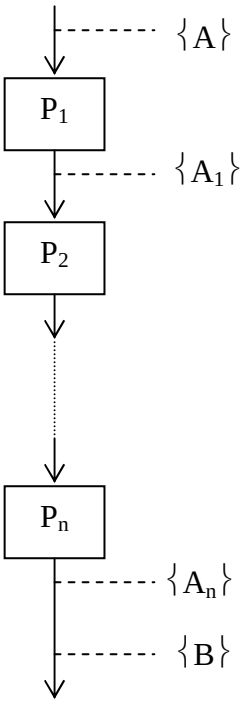
....

P_n biến đổi $\{A_{n-1}\}$ thành $\{A_n\}$

Và dựa vào quy tắc toán học, $\{A_n\}$ có thể suy ra $\{B\}$ thì ta có thể nói rằng P là đúng với cái vào $\{A\}$ và cái ra $\{B\}$. Lúc này ký hiệu $\{A\}P\{B\}$ hay $\{A\} \overset{P}{=>} \{B\}$.

Cần chú ý rằng $\{A\} \overset{P}{=>} \{B\}$ là khác với $\{A\} \overset{L}{=>} \{B\}$:mệnh đề {A} suy diễn ra mệnh đề {B} dựa vào các quy tắc toán học.

Nói cách khác, để chứng minh P là đúng, ta chứng minh theo sơ đồ sau:



$\{A\}$ P_1 $\{A_1\}$

$\{A_1\}$ P_2 $\{A_2\}$

.....

.....

$\{A_{n-1}\}P_n\{A_n\}$

$\{A_n\} \overset{L}{=>} \{B\}$

Ở đây, cần để ý là tính chất $\{A\}$ và tính chất $\{B\}$ có thể không liên quan đến nhau.

Ví dụ 1: Cho mệnh đề dữ liệu vào {A: x,y∈R; 0<x<1}, dữ liệu ra {B: x,y∈R; x>y+3}

Và đoạn trình $P = P_1 \cup P_2 \cup P_3 \cup P_4$ như sau:

x:=1/x+1; (P_1)

y:=y+1; (P_2)

x:=x+2; (P_3)

x:=x+y; (P_4)

Lúc này ta có dãy biến đổi tính chất dữ liệu vào/ ra như sau:

$\{A\}\ P_1\{A_1: x,y\in R;\ x>2\}$

$\{A_1\}P_2\{A_2: x,y\in R;\ x>2\}$

$\{A_2\}P_3\{A_3: x,y\in R;\ x>4\}$

$\{A_3\}P_4\{A_4: x,y\in R;\ x>y+4\}$

và $\langle A_4\rangle \overset{L}{\Rightarrow} \langle B\rangle$

Vậy ta có kết luận {A}P{B} hay nói cách khác là P đúng với dữ liệu vào {A} và dữ liệu ra {B}.

Cần để ý rằng khí ta có dãy biến đổi tính chất dữ liệu vào và ra như sau:

$\langle A\rangle\ P_1\ \langle A_1\rangle$

$\langle A_1\rangle\ P_2\ \langle A_2\rangle$

.....

.....

$\langle A_{n-1}\rangle P_n \langle A_n\rangle$

$\langle A_n\rangle \overset{L}{\not\Rightarrow} \langle B\rangle$

Thì chưa thể kết luận được điều gì vì còn tuỳ thuộc vào các mệnh đề trung gian thu được $\{A_1\},\{A_2\},....\{A_n\}$ là đã "mạnh nhất" hay chưa.

Xét ví dụ đã cho ở trên, ta có dãy biến đổi như sau:

$\{A\}\ P_1\{A'_1: x,y\in R;\ x>0\}$

$\{A'_1\}P_2\{A'_2: x,y\in R;\ x>0\}$

$\{A'_2\}P_3\{A'_3: x,y\in R;\ x>2\}$

$\{A'_3\}P_4\{A'_4: x,y\in R;\ x>y+2\}$

Rõ ràng ta có: $\langle A'_4\rangle \overset{L}{\not\Rightarrow} \langle B\rangle$ nhưng theo trên ta vẫn có kết luận {A}P{B}.

Trong trường hợp này, ta thấy các mệnh đề $\{A'_1\}\{A'_2\}\{A'_3\}\{A'_4\}$ rõ ràng là các mệnh đề hệ quả của các mệnh đề $\{A_1\}\{A_2\}\{A_3\}\{A_4\}$.

Ví dụ 2: Cho mệnh đề dữ liệu vào {A: x,y∈N; x=3y}, đoạn trình P =$P_1 \cup P_2$ như sau:

x:=x+5; (P_1)

y:=y+5; (P_2)

và mệnh đề dữ liệu ra {B: x,y∈R; x=3y}. Ở đây, rõ ràng ta có $\{A\} \overset{P}{\neq>} \{B\}$

4.2. Hệ tính chất Hoare

1. Tính chất 1: Tính chất của cấu trúc tuần tự

Nếu mệnh đề $\{A\}$ sau khi chịu tác động của khối cấu trúc điều khiển P ta được $\{B\}$ và mệnh đề $\{B\}$ sau khi chịu tác động của cấu trúc điều khiển Q ta được $\{C\}$ thì $\{A\}$ chịu tác động tuần tự P,Q sẽ thu được $\{C\}$

Hay nói cách khác, đây chính là tiên đề về dãy thao tác: Nếu $\{A\}$ P $\{B\}$ và $\{B\}$ Q $\{C\}$ thì $\{A\}$ P,Q $\{C\}$

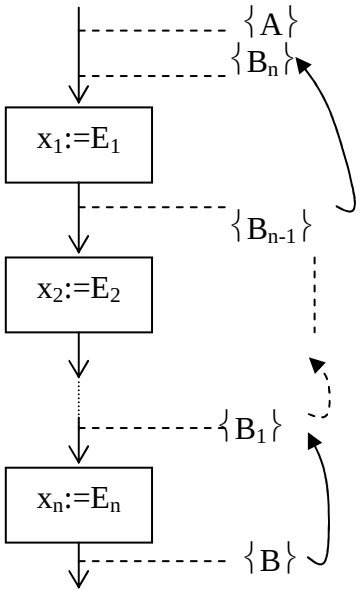
2. Tính chất 2: tính chất của phép gán

Điều kiện để có mệnh đề $\{B\}$ sau khi thực hiện lệnh gán x: = E (với E là một biểu thức) từ mệnh đề {A} thì trước đó ta phải có {A} suy dẫn được ra {B[x|E]}.

Mệnh đề {B[x|E]} là mệnh đề thu được từ {B} bằng phép thay thế mọi xuất hiện của x trong {B} bởi E. Tức là: $\{A\}$ x: = E $\{B\}$ thì $\{A\} \overset{L}{=>} \{B[x|E]\}$

- *Kỹ thuật lần ngược của tiên đề gán*

Cho đoạn trình P gồm n phép gán $x_1:=E_1$; $x_2:=E_2$;.....$x_n:=E_n$; để {A}P{B} thì ta phải có $\{A\} \overset{L}{=>} \{B_n\}$. Trong đó $\{B_n\}$ được xác định như sau



Trong đó các mệnh đề $\{B_i\}$ được xác định như sau:

$\{B_1\}$ là mệnh đề $\{B[x_n|E_n]\}$

$\{B_{n-1}\}$ là mệnh đề $\{B_{n-2}[x_2|E_2]\}$

$\{B_n\}$ là mệnh đề $\{B_{n-1}[x_1|E_1]\}$

Trong trường hợp $\{A\} \overset{L}{\neq} \{B_n\}$ thì ta nói P là có lỗi.

Ví dụ 3: (Xét ví dụ 1) Cho mệnh đề dữ liệu vào $\{A: x,y \in R; 0<x<1\}$,

Đoạn trình $P = P_1 \cup P_2 \cup P_3 \cup P_4$ như sau:

x:=1/x+1; (P_1)

y:=y+1; (P_2)

x:=x+2; (P_3)

x:=x+y; (P_4)

và mệnh đề dữ liệu ra $\{B: x,y \in R; x>y+3\}$. Hãy khảo sát $\{A\}P\{B\}$ hay không?

Ta có

$\{B[x|x+y]\} \equiv \{B_1 : x+y, y \in R; x+y>y+3\}$

$\{B_1[x|x+2]\} \equiv \{B_2 : (x+2)+y, y \in R; (x+2)+y>y+3\}$

$\{B_2[y|y+1]\} \equiv \{B_3 : (x+2)+(y+1),(y+1) \in R;\ (x+2)+(y+1)>(y+1)+3\}$

$\{B_3[x|1/x+1]\} \equiv \{B_4 : ((1/x+1)+2)+(y+1),(y+1) \in R;\ ((1/x+1)+2)+(y+1)>(y+1)+3\}$

Rõ ràng ta có $\{A\} \overset{L}{\Rightarrow} \{B_4\}$., nên {A}P{B}.

3. Tính chất 3- Tính chất của cấu trúc chọn lựa

i. Với mệnh đề dữ liệu vào {A}, mệnh đề dữ liệu ra {B}, biểu thức logic E, và đoạn trình P. Nếu ta có {A, E}P{B} và $\{A,!E\} \overset{L}{\Rightarrow} \{B\}$ thì ta nói rằng mệnh đề {A} và {B} tuân theo cấu trúc rẽ nhánh dạng khuyết với cấu trúc P và điều kiện lựa chọn E; tức là: {A} *if* E *then* P*;* {B}.

ii. Với mệnh đề dữ liệu vào {A}, mệnh đề dữ liệu ra {B}, biểu thức logic E, và các đoạn trình P, Q. Nếu ta có {A, E}P{B} và {A,!E}Q{B} thì ta nói rằng mệnh đề {A} và {B} tuân theo cấu trúc rẽ nhánh dạng đủ với cấu trúc P, Q và điều kiện lựa chọn E; tức là: {A} *if* E *then* P *else* Q*;* {B}.

Ví dụ 4: Cho mệnh đề dữ liệu vào {A: x,y,q,r∈N, x=qy+r, 0≤r<2y}, đoạn trình P như sau:

```
If y≤r then
    Begin
        q:=q+1;
        r:=r-y;
    End;
```

Và mệnh đề dữ liệu ra {B: x,y,q,r∈N, x=qy+r, 0≤r<y}. Hãy xem {A}P{B}?

Áp dụng tính chất của phép gán, ta có:

i. {A,E: x,y,q,r∈N, x=qy+r, 0≤ r<2y, y≤ r}q:=q+1;r:=r-y;{B}

ii. {A,!E: x,y,q,r∈ N, x=qy+r, 0≤ r<2y, y>r}=Þ{B}

do đó suy ra {A}P{B}.

4. Tính bất biến của chương trình

Cho mệnh đề dữ liệu vào {A} và đoạn trình P. Nếu ta có {A}P{A} thì ta nói rằng tính chất dữ liệu của mệnh đề {A} không thay đổi khi chịu sự tác động của đoạn trình P và lúc này người ta nói rằng mệnh đề {A} là bất biến đối với P, tức ta có: {A}P {A}.

Ví dụ 5: Ta có mệnh đề {A: x∈ R, x>0} là bất biến đối với đoạn trình P: x:=x*x; vì ta có {A}P{A}.

5. Tính chất 4: Tính chất của cấu trúc lặp

Cho mệnh đề dữ liệu vào {A}, biểu thức logic E và đoạn trình P. Nếu mệnh đề {A} tuân theo cấu trúc lặp P với điều kiện lặp E thì mệnh đề {A} sẽ bất biến đối với P trong điều kiện E, tức là {A,E}P{A}, kết thúc vòng lặp ta có mệnh đề {A,!E}. Lúc này ta viết: {A} *while* E *do* P; {A,!E}.

Ví dụ 6: Cho x,y,z là 3 số nguyên không âm. Hãy viết chương trình để tính z=xy, biết rằng x,y được nhập từ bàn phím. Hãy khẳng định tính đúng của chương trình.

Ta có đoạn trình như sau:

Vào: x,y,z∈ N; x=a; y=b;

Ra: x,y,z∈ N; z=ab;

Chương trình P được viết:

```
z:=0;
while x>0 do
        Begin
                If  (x mod 2)≠0 then z:=z+y;
                x=x div 2;
                y:=y*2;
```

End;

Return z;

Ta cần phải khẳng định chương trình trên đúng với yêu cầu đặt ra.

Thật vậy, gọi mệnh đề thể hiện tính chất dữ liệu vào của chương trình {A} và mệnh đề thể hiện tính chất dữ liệu ra cần có {B}, ta có

{A: x,y,z∈ N; x=a; y=b;} và {B: x,y,z∈ N; z=ab;}

Ta cần chứng tỏ {A}P {B}.

+ Xét mệnh đề {C: x,y,z∈ N; ab=z+xy;}

+ Ta có {A} z:=0;{C}

+ Để chứng tỏ {C} là bất biến của đoạn trình

while x>0 *do*

Begin

If (x mod 2)≠0 *then* z:=z+y;

x=x div 2;

y:=y*2;

End;

Ta cần có: {C,E: x,y,z∈ N; ab=z+xy;x>0}Q{C}, với đoạn trình Q như sau:

If (x mod 2)=0 *then* z:=z+y;

x=x div 2;

y:=y*2;

Theo tính chất của phép gán, ta có:

$\{C_1\}\equiv\{C[y|y*2]: x,y*2,z\in N; ab=z+x(y*2);\}$

$\{C_2\}\equiv\{C_1[x|(x \text{ div } 2)]: (x \text{ div } 2),y*2,z\in N; ab=z+(x \text{ div } 2)(y*2);\}$

Nên cần chứng tỏ:

{C,E: x,y,z∈ N; ab=z+xy;x>0} *If* (x mod 2)≠0 *then* z:=z+y; $\{C_2\}$

Dễ dàng ta có

i. {C,E,F: x,y,z∈ N; ab=z+xy;x>0,(x mod 2)≠0} z:=z+y {C_2}; và

ii..{C,E,!F: x,y,z∈ N; ab=z+xy;x>0,(x mod 2)=0} $\overset{L}{=>}${C_2};

Vậy {C} là bất biến của Q. Nên kết thúc Q, ta có mệnh đề {C,!E}.

+ Dễ dàng chứng tỏ: {C,!E}$\overset{L}{=>}${B}

Vậy ta có {A}P{B}, hay chương trình trên là đúng.

Để ý rằng: do {A,E}P{A} nên trong trường hợp {A}$\overset{L}{=>}$E thì vòng lặp là vô hạn và không tồn tại mệnh đề {A, !E}.