Software Specifications
Specifications

Cain Susko

Queen's University
School of Computing

March 7, 2022

Verifying Specifications

given that the entries A[0]...A[max-1] are known to exist:

```
ASSERT( 0 <= n <= max && A == A0 ) /* pre-condition */

{int i
A[n] = x; i=0;
while (S[i] !+ x) i++;
present = (i<n)

ASSERT( (persent iff x in A[0:n-1]) &&
ForAll (i=0; i<n) A[i] == A0[i] ) /* post-condition */
```

So now, we want to create a systematic way of verifying if specifications hold. for equalities, we can verify them by using the logic:

$$V == I : \{V = E_j\} \equiv V == [E](V \mapsto I)$$

but this forward logic is very convoluted. A better way may be to reason *backwards*. Thus, based on the post condition, determine the most general pre-contition that guarantees that the post-condition holds after assignment:

$$[Q](V \mapsto E)\{V = E_j\}\ Q$$

This is known as the Hoirre Axiom for finding pre-conditons. assertion obtained by Q by relacing occurences of V with E.
Note: we must be careful when substituting quantified variables (will cover later).

Examples

- $P\ \ \{x = 1_j\}\ \ x == 1$
  $P\ =\ 1 == 1$ pre-condition is true

- $P\ \ \{x = 1_j\}\ \ x == 0$
  $P\ =\ 1 == 0$ pre-condition is false

- $P\ \ \{x = y + z_j\}\ \ x * x > y$
  $P\ =\ (y + z) * (y + z) > y$ pre-condition is unknown if true or false

Issues With Substitution

there are a few special actions one should take in order to avoid problems with substitution using the Hoirre Axiom:

i Add parenthesis when neccesary

ii Only free occurrences of a variable are substituted

iii As a result of a substitution, free occurrences of a variable should not become bound. If neccessary, we should change the name of the bound variable

Examples

i $P \ \{z = x + y_j\} \ z * z > y$
$P \ = \ (x + y) * (x + y) > y$

ii $P \ \{z = x + y_j\} \ Exists(z = 0, z < 50) \ z == x + y$
$P \ = \ Exists(z = 0, z < 50) \ z == x + y$

iii $P \ \{z = x + y_j\} \ Exists(y = 0, y < 50) \ x * y == z$ Note: we rename the bound variable y_j to a
$P \ = \ Exists(a = 0, a < 50) \ x * a == x + y$

note: we cannot rename free variables but we can rename bound variables.

Recall

please Recall bound and unbound variables (from cisc204).
given:

$$\exists(x = 0, x < w)\exists(z = a, z < b) \ [x * y \geq 2 * z + w]$$

where the variables are:

Free x, z

Bound w, a, b, y