6 – Лаборатория иши

VCGen билан дастурий маҳсулотларни текшириш

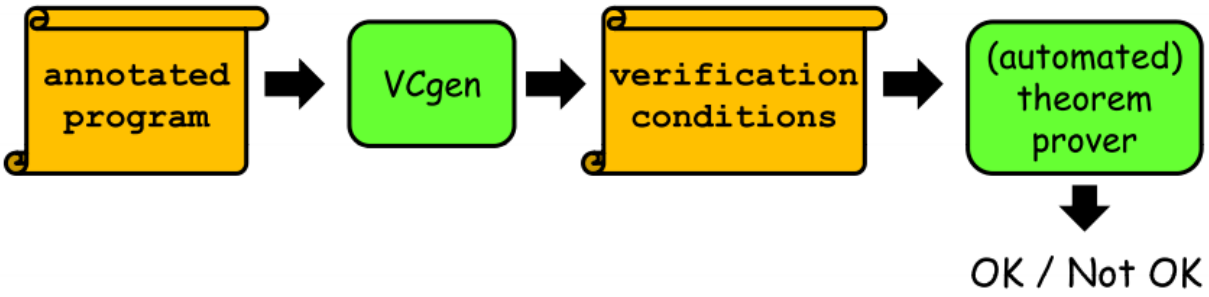
Ишдан мақсад: Жава дастурлаш тилида OpenJMLдан фойдаланган ҳолда дастурий кодларни текшириш.

Назарий қисм

Дастурий таъминот текширувчилари (program verification) – дастур қаноатлантирган баъзи хусусиятларнинг математик тасдиғини амалга оширади. Яъни, кириши мумкин бўлган кириш қийматлар, барча бўлиши мумкин бўлган оқимлар ва ҳак. Саноатда тестлаш одатда текшириш каби маълум. Сабаби, тестлашда баъзи ҳолатлар учун дастурий таъминот юкланиб кўрилади. Бу жараён кам вақт талаб этсада, тўлиқ текширишни амалга оширмайди.

VCGen (Verification condition generation) билан дастурни текшириш. Одатда кўплаб стандарт дастурларни текширишда VCGen дан фойдаланилади:

- Дастур хусусиятлар билан изоҳланади;
- VCGen текшириш шартлари деб аталувчи мантиқий хусусиятларни (specification) генерация қилади;
- Агар бу текшириш шартлари тўғри бўлса, изоҳлар (annotation) тўғри ва хусусиятлар дастурни қаноатлантиради.



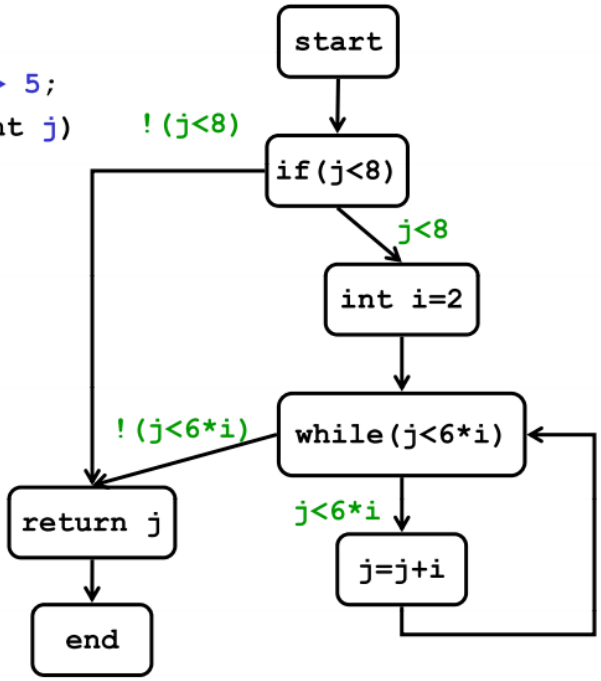
VCGen ёрдамида текширишга қуйидаши мисол берилган:

```
//@ requires true;
//@ ensures \result > 5;
public int example(int j)
{
  if (j < 8) {
     int i = 2;
     while (j < 6*i){
       j = j + i;
     }
  }
  return j;
}
```

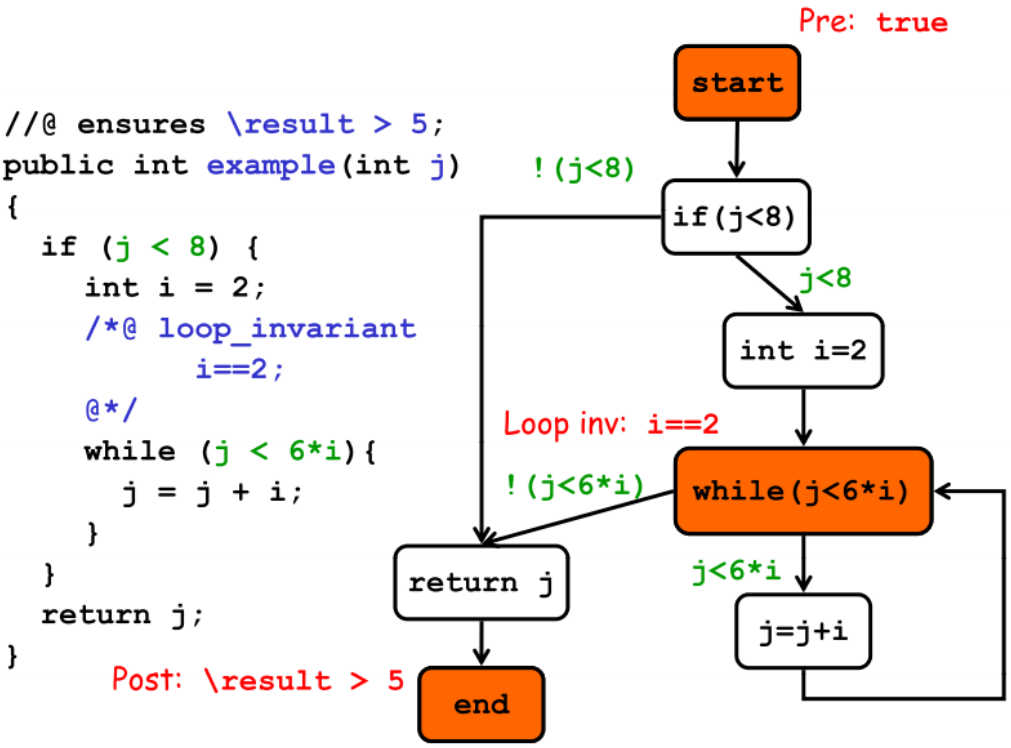
Ушбу мисолни VCGen билан текшириш қуйидагича амалга оширилади:

- **График кўринишда**

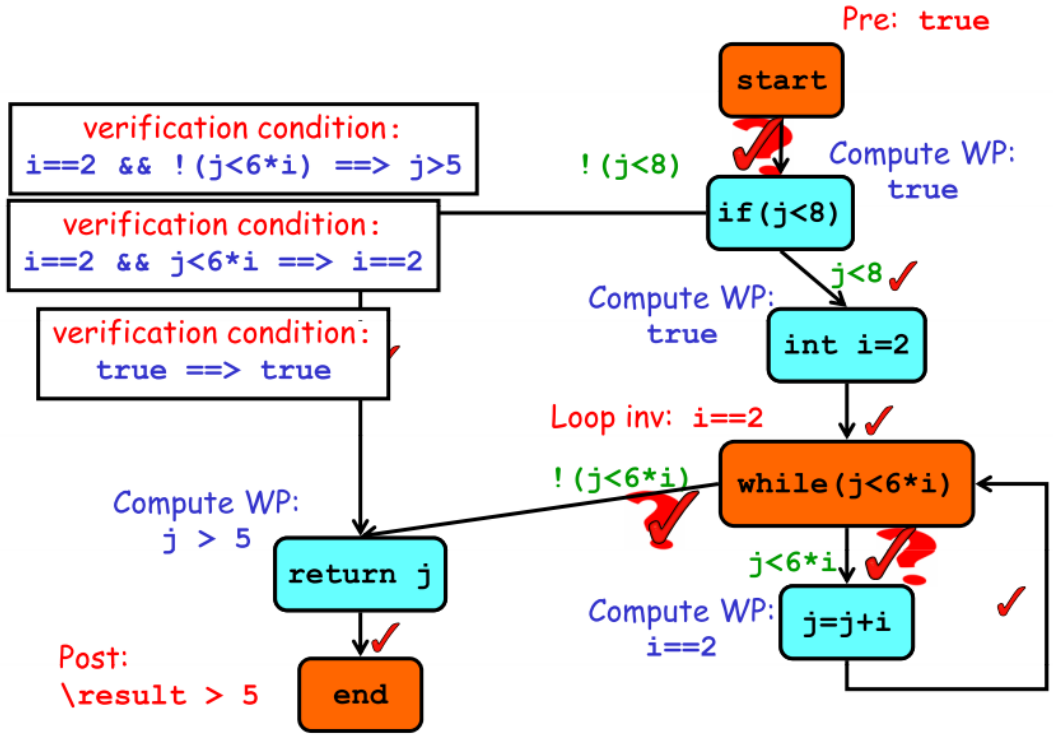
```
//@ ensures \result > 5;
public int example(int j)
{
  if (j < 8) {
     int i = 2;
     while (j < 6*i){
       j = j + i;
     }
  }
  return j;
}
```



- **Тасдиқларни қўшиш**



- **Текшириш ҳолатларини ҳосил қилиш ва текшириш**



Наоре учлиги. Бу учлик қуйидагича ифойдаланади: { P } S { Q }. Бу ерда S – буйруқ, P – дастлабки шарт – S буйруқ бажарилгунга қадар ҳолат ва Q буйруқ бажарилгандан кейинги ҳолат – кейинги шарт.

Бирор хатолик юз бермаган ҳолда P ҳолатда Q ҳолатга ўтиш бажарилади. Ушбу учлигга мисол:

- ✓ {a = 2} b := a + 3; {b > 0}
- ✓ {a = 2} b := a + 3; {b = 5}
- ✓ {a > 3} b := a + 3; {a > 0}
- ✓ {a = 2} b := a * a; {b > 0}

Ушбу учликга асосланган VCC воситаси C кодларни таҳлиллаш учун Visual Studio дастурий пакетида фойдаланилади (онлайн - http://rise4fun.com/Vcc/hello). Java дастурлаш тиллари учун эса Java Modeling Language (JML)дан фойдаланилади (https://rise4fun.com/OpenJMLESC).

Амалий қисм

JML оддий Java дастурлаш тилларида ёзилган кодларда изоҳлар қўшиш орқали текширишни амалга оширади. JML изоҳлари Java изоҳларидан фарқли *//@ <JML specification>* ёки */*@ <JML specification> @*/* кўринишда қўйилади.

Асосий JML нинг калит сўзлари қуйидагидан иборат:

requires – усулнинг дастлабки шартини ифодалаш

ensures – усулнинг кейинги шартини ифодалаш

signals - берилган кутилма усул томонидан қайтарилган ҳолдаги кейинги шартни ифодалайди.

signals_only – дастлабки шартлар бажарилган вақтда қандай кутилмалар (Exception) қайтарилишини кўрсатади.

assignable – усул томонидан қайси соҳа қўйилганлигини аниқлайди.

invariant – класснинг инвараиантлик хусусиятини ифодалайди.

loop_invariant – цикл учун цикл инварантини ифойдалайди.

also – хусусиятарни бирлаштириш учун фойдаланилади.

assert - JML assertion ни аниқлайди.

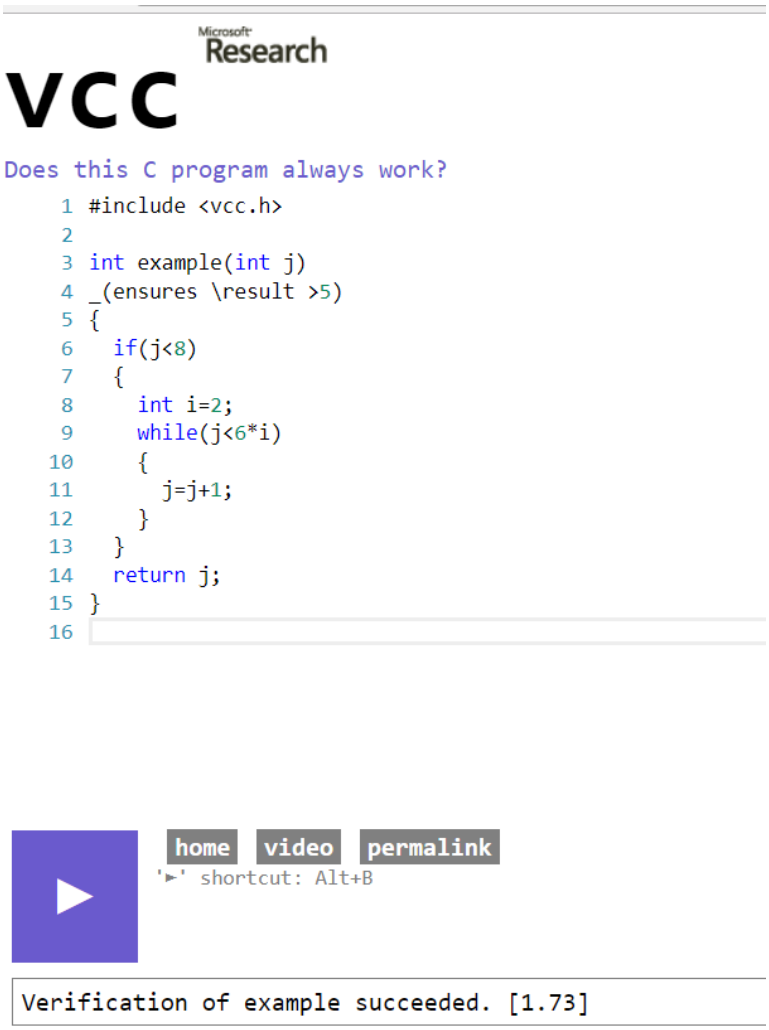
spec_public - protected ёки private ни аниқлайди.

Қуйида VCGen иловасини C дастурлаш тили учун ёзилган изоҳлари келтирилган:

1. Наъмуна

```
#include <vcc.h>
```

```
int example(int j)
_(ensures \result >5)
{
  if(j<8)
  {
    int i=2;
    while(j<6*i)
    {
      j=j+1;
    }
  }
  return j;
}
```



2. Наъмуна

```
#include <vcc.h>

int max(int a, int b)
  _(ensures \result == (a > b ? a : a))
{
    if (a > b) return a;
    return b; // fails against post condition
```

```
}
```

		Description
⊗	1	Post condition '\result == (a > b ? a : a)' did not verify.
⊗	2	(related information) Location of post condition.

```
Verification of max failed. [2.91]
snip(7,5) : error VC9501: Post condition '\result == (a > b ? a : a)' did not verify.
snip(4,13) : error VC9599: (related information) Location of post condition.
Verification errors in 1 function(s)
Exiting with 3 (1 error(s).)
```

```
#include "vcc.h"

int max(int a, int b)
  _(ensures \result == (a > b ? a : b))  // fixed specification
{
    if (a > b) return a;
    return b;
}
```

```
Verification of max succeeded. [1.73]
```

```
#include <vcc.h>

int succ(int i)
_(ensures \result == i+1)
{
    return i+1; // fails with overflow
}
```

		Description
⊗	1	i+1 might overflow.

```
Verification of succ failed. [1.70]
snip(7,12) : error VC8004: i+1 might overflow.
Verification errors in 1 function(s)
Exiting with 3 (1 error(s).)
```

```
#include <vcc.h>
#include <limits.h>
int succ(int i)
_(requires i<INT_MAX)
_(ensures \result == i+1)
{
    return i+1;
}
```

```
Verification of succ succeeded. [2.17]
```

Назорат саволлари

1. Ихтиёрий бешта Java код яратинг ва уларга JML изоҳларини киритинг.
2. JML изоҳларни ишлагини билиш учун турли қийматлар киритинг ва олинган натижаларни ҳисоботда акс эттиринг.