Software Verification

Introduction to CEGAR/Predicate Abstraction

Ahmed Rezine

IDA, Linköpings Universitet

Spring 2021

Outline

Verification and approximations

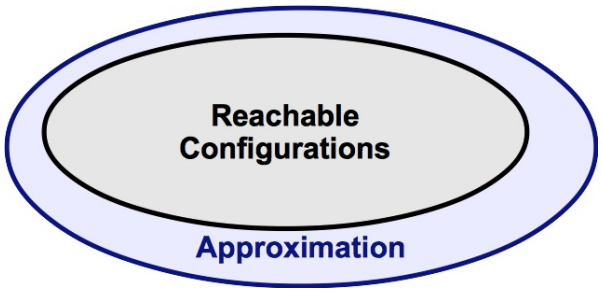
Predicate abstraction and CEGAR

Further readings

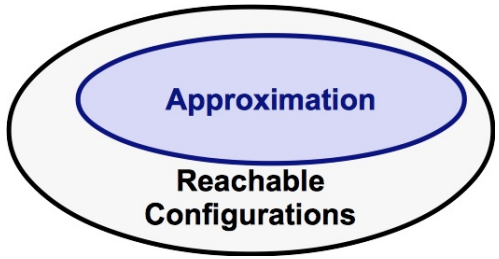
Outline

Verification and approximations

- The idea is to come up with efficient approximations to give correct answers in as many cases as possible.



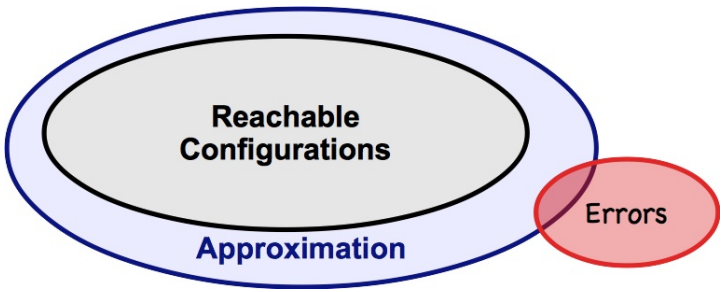
Over-approximation



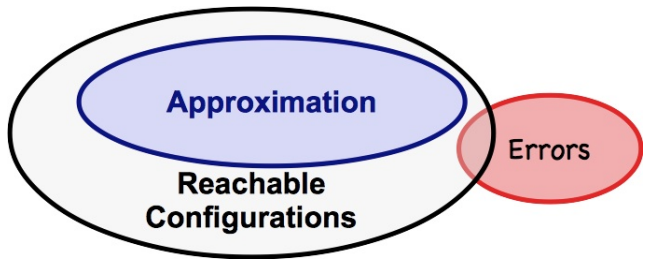
Under-approximation

Program verification and the price of approximations

- A sound analysis cannot give **false negatives**
- A complete analysis cannot give **false positives**



False Positive



False Negative

Approaches

- We discussed:
  - Explicit/symbolic model checking
  - Symbolic Execution relying on SMT solvers
  - Deductive frameworks with Hoare triples
- Last time: abstract interpretation: define an abstract domain and abstract transformers.
- Today: define an abstract domain iteratively

Outline

An example

```
state {
  enum {Locked, Unlocked}
  s = Unlocked;
}

KeAcquireSpinLock.entry{
  if(s == Locked)
    abort;
  else
    s= Locked;
}

KeReleaseSpinLock.entry{
  if(s == Unlocked)
    abort;
  else
    s= Unlocked;
}
```

An example

```
state {
  enum {Locked, Unlocked}
  s = Unlocked;
}

KeAcquireSpinLock.entry{
  if(s == Locked)
    abort;
  else
    s= Locked;
}

KeReleaseSpinLock.entry{
  if(s == Unlocked)
    abort;
  else
    s= Unlocked;
}
```

```
do{

  KeAquireSpinLock();

  nPacketsOld= nPackets;

  if(request){

    request = request->next;

    KeReleaseSpinLock();

    nPackets++;
  }

}while(nPackets != nPacketsOld);

KeReleaseSpinLock();
```

An example: Refinement

```
do{
  KeAquireSpinLock();

  if( * ){

    KeReleaseSpinLock();

  }
}while( * );
KeReleaseSpinLock();
```

```
do{
  KeAquireSpinLock();
  nPacketsOld= nPackets;
  if(request){
    request = request->next;
    KeReleaseSpinLock();
    nPackets++;
  }
}while(nPackets != nPacketsOld);
KeReleaseSpinLock();
```

Acquire the lock twice seems possible. Spurious?

An example: Refinement

```
do{
  KeAquireSpinLock();

  if( * ){

    KeReleaseSpinLock();

  }
}while( * );
KeReleaseSpinLock();
```

```
do{
  KeAquireSpinLock();
  nPacketsOld= nPackets; //b= true
  if(request){
    request = request->next;
    KeReleaseSpinLock();
    nPackets++; //b= b? false; *
  }
}while(nPackets != nPacketsOld); // !b
KeReleaseSpinLock();
```

The predicate b representing `nPacketsOld==nPackets` seems important.

An example: Refinement

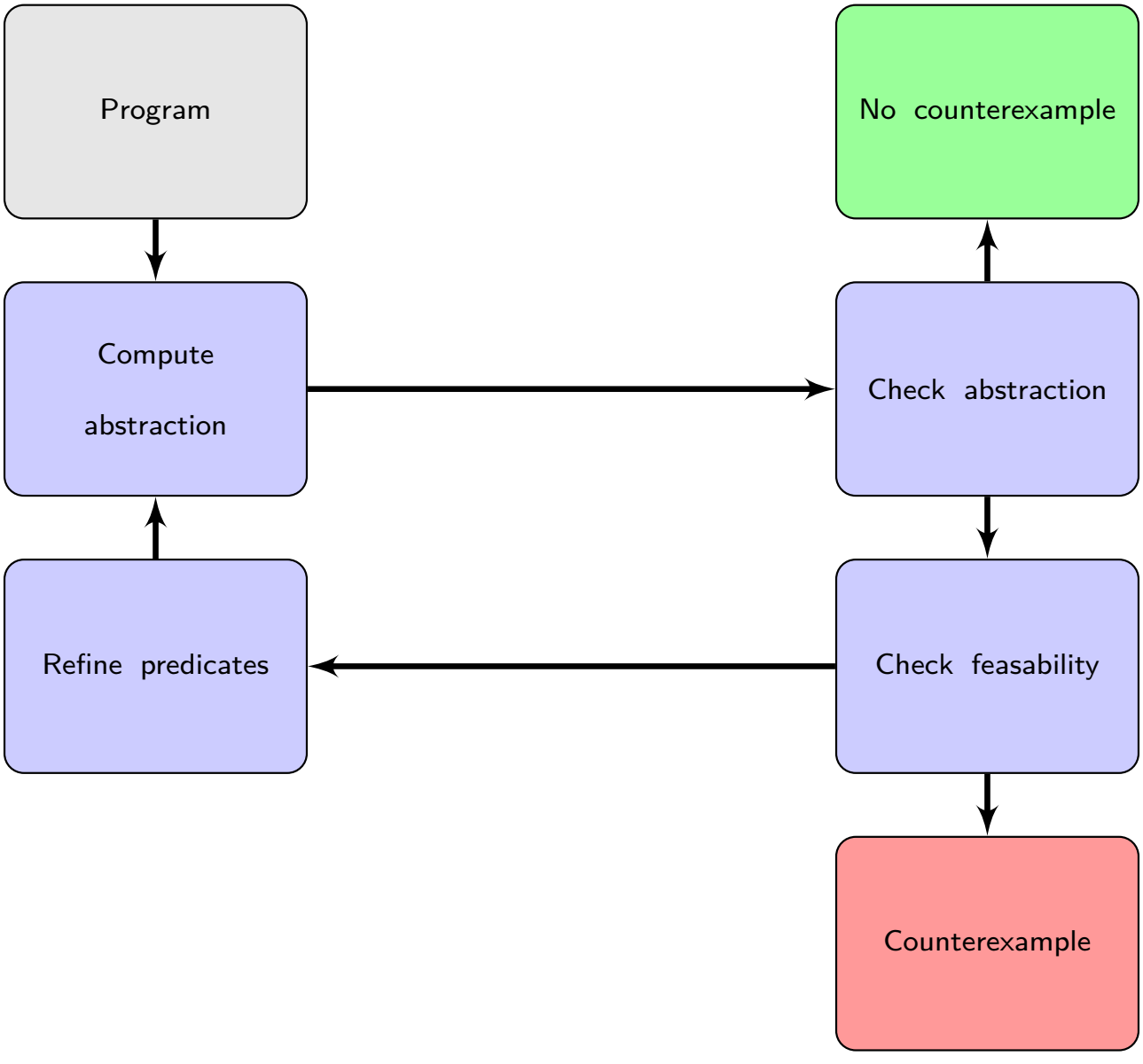
```
do{
  KeAquireSpinLock();
  b= true;
  if( * ){


    KeReleaseSpinLock();
    b= b? false: *;
  }
}while( !b );
KeReleaseSpinLock();
```

```
do{
  KeAquireSpinLock();
  nPacketsOld= nPackets; //b= true
  if(request){
    request = request->next;
    KeReleaseSpinLock();
    nPackets++; //b= b? false; *
  }
}while(nPackets != nPacketsOld); //!b
KeReleaseSpinLock();
```

The predicate b representing `nPacketsOld==nPackets` seems important.

An example: CEGAR



Counterexample-guided abstraction refinement

Outline

Further readings

- Slam. https://www.microsoft.com/en-us/research/project/slam/. Accessed: 2021-01-22.
- Satabs. predicate abstraction using sat. https://www.cprover.org/satabs/. Accessed: 2021-01-22.
- Cpachecker. the configurable software-verification platform. https://cpachecker.sosy-lab.org/doc.php. Accessed: 2021-01-22.
- T. Ball, R. Majumdar, T. Millstein, and S. K. Rajamani. Automatic predicate abstraction of c programs. PLDI01.
- D. Beyer, T. A. Henzinger, R. Jhala, and R. Majumdar. The software model checker blast. STTT07.
- E. Clarke, O. Grumberg, S. Jha, Y. Lu, and H. Veith. Counterexample-guided abstraction refinement. CAV00.
- S. Graf and H. Saidi. Construction of abstract state graphs with pvs. CAV97.