Algorithmic Logic-Based Verification with SeaHorn

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Arie Gurfinkel with Teme Kahsai and Jorge A. Navas

based on work with Anvesh Komuravelli, and Nikolaj Bjørner
Automated Software Analysis

Program → Automated Analysis

Correct
Incorrect

Software Model Checking with Predicate Abstraction
e.g., Microsoft’s SDV

Abstract Interpretation with Numeric Abstraction
e.g., ASTREE, Polyspace
Turing, 1936: “undecidable”
How can one check a routine in the sense of making sure that it is right?

The programmer should make a number of definite assertions which can be checked individually, and from which the correctness of the whole programme easily follows.

Alan M. Turing. “Checking a large routine”, 1949
Three-Layers of a Program Verifier

Compiler
• compiles surface syntax a target machine
• embodies syntax with semantics

Verification Condition Generator
• transforms a program and a property to a verification condition in logic
• employs different abstractions, refinements, proof-search strategies, etc.

Automated Theorem Prover / Reasoning Engine
• discharges verification conditions
• general purpose constraint solver
• SAT, SMT, Abstract Interpreter, Temporal Logic Model Checker,…
SeaHorn

A fully automated verification framework for LLVM-based languages.

http://seahorn.github.io
SeaHorn Verification Framework

Arie Gurfinkel
Software Engineering Institute
Carnegie Mellon University

Temesghen Kahsai
Carnegie Mellon University
NASA Ames

Jorge A. Navas
SGT
NASA Ames
The Plan

Introduction

Architecture and Usage

Demonstration

Constrained Horn Clauses as an Intermediate Representation

From Programs to Logic
  • generating verification conditions

Program Transformations for Verification

Solving Constrained Horn Clauses
  • synthesizing inductive invariants and procedure summaries

Conclusion
SeaHorn Verification Framework

Key Features

- LLVM front-end(s)
- Constrained Horn Clauses to represent Verification Conditions
- Comparable to state-of-the-art tools at SV-COMP’15

Goals

- be a state-of-the-art Software Model Checker
- be a framework for experimenting and developing CHC-based verification
Related Tools

CPAChecker
• Custom front-end for C
• Abstract Interpretation-inspired verification engine
• Predicate abstraction, invariant generation, BMC, k-induction

SMACK / Corral
• LLVM-based front-end
• Reduces C verification to Boogie
• Corral / Q verification back-end based on Bounded Model Checking with SMT

UFO
• LLVM-based front-end (partially reused in SeaHorn)
• Combines Abstract Interpretation with Interpolation-Based Model Checking
• (no longer actively developed)
SeaHorn Philosophy

Build a state-of-the-art Software Model Checker
• useful to “average” users
  – user-friendly, efficient, trusted, certificate-producing, …
• useful to researchers in verification
  – modular design, clean separation between syntax, semantics, and logic, …

Stand on the shoulders of giants
• reuse techniques from compiler community to reduce verification effort
  – SSA, loop restructuring, induction variables, alias analysis, …
  – static analysis and abstract interpretation
• reduce verification to logic
  – verification condition generation
  – Constrained Horn Clauses

Build reusable logic-based verification technology
• “SMT-LIB” for program verification
SeaHorn Usage

> sea pf FILE.c

Outputs sat for unsafe (has counterexample); unsat for safe

Additional options

- --cex=trace.xml outputs a counter-example in SV-COMP’15 format
- --show-invars displays computed invariants
- --track={reg,ptr,mem} track registers, pointers, memory content
- --step={large,small} verification condition step-semantics
  - small == basic block, large == loop-free control flow block
- --inline inline all functions in the front-end passes

Additional commands

- sea smt -- generates CHC in extension of SMT-LIB2 format
- sea clp -- generates CHC in CLP format (under development)
- sea lfe-smt -- generates CHC in SMT-LIB2 format using legacy front-end
Verification Pipeline

front-end

```
clang | pp | ms | opt | horn
```

- compile
- pre-process
- optimize
- mixed semantics
- VC gen & solve
From Programming to Modeling

Extend C programming language with 3 modeling features

Assertions

• assert(e) – aborts an execution when e is false, no-op otherwise
  
  ```c
  void assert (_Bool b) { if (!b) abort(); }
  ```

Non-determinism

• nondet_int() – returns a non-deterministic integer value
  
  ```c
  int nondet_int () { int x; return x; }
  ```

Assumptions

• assume(e) – “ignores” execution when e is false, no-op otherwise
  
  ```c
  void assume (_Bool e) { while (!e); }
  ```
Constrained Horn Clauses

INTERMEDIATE REPRESENTATION
Constrained Horn Clauses (CHC)

A Constrained Horn Clause (CHC) is a FOL formula of the form

$$8 V . (Á \forall p_1[X_1] \forall \ldots \forall p_n[X_n] \rightarrow h[X]),$$

where

• A is a background theory (e.g., Linear Arithmetic, Arrays, Bit-Vectors, or combinations of the above)
• Á is a constrained in the background theory A
• $p_1, \ldots, p_n, h$ are n-ary predicates
• $p_i[X]$ is an application of a predicate to first-order terms
int $x = 1$;
int $y = 0$;
while ($\ast$) {
    $x = x + y$;
    $y = y + 1$;
}
assert($x \geq y$);

\begin{itemize}
    \item \(l_0:\)
        \begin{align*}
            x &= 1 \\
            y &= 0
        \end{align*}
    \item \(l_1 : b_1 = \text{nondet()}\)
    \item \(l_2 :\)
        \begin{align*}
            x &= x + y \\
            y &= y + 1
        \end{align*}
    \item \(l_3 :\)
        \begin{align*}
            b_2 &= x \geq y \\
            x' &= x + y \\
            y' &= y + 1
        \end{align*}
    \item \(l_4 :\)
    \item \(l_{\text{err}} :\)
\end{itemize}

\begin{itemize}
    \item \(\langle 1 \rangle p_0.\)
    \item \(\langle 2 \rangle p_1(x, y) \leftarrow p_0, x = 1, y = 0.\)
    \item \(\langle 3 \rangle p_2(x, y) \leftarrow p_1(x, y).\)
    \item \(\langle 4 \rangle p_3(x, y) \leftarrow p_1(x, y).\)
    \item \(\langle 5 \rangle p_1(x', y') \leftarrow p_2(x, y), x' = x + y, y' = y + 1.\)
    \item \(\langle 6 \rangle p_4 \leftarrow (x \geq y), p_3(x, y).\)
    \item \(\langle 7 \rangle p_{\text{err}} \leftarrow (x < y), p_3(x, y).\)
    \item \(\langle 8 \rangle p_4 \leftarrow p_4.\)
    \item \(\langle 9 \rangle \bot \leftarrow p_{\text{err}}.\)
\end{itemize}
CHC Terminology

Rule

\[ h[X] \models p_1[X_1], ..., p_n[X_n], \models. \]

Query

\[ \text{false} \models p_1[X_1], ..., p_n[X_n], \models. \]

Fact

\[ h[X] \models \models. \]

Linear CHC

\[ h[X] \models p[X_1], \models. \]

Non-Linear CHC

\[ h[X] \models p_1[X_1], ..., p_n[X_n], \models. \]

for \( n > 1 \)
CHC Satisfiability

A model of a set of clauses $\Gamma$ is an interpretation of each predicate $p_i$ that makes all clauses in $\Gamma$ valid.

A set of clauses is **satisfiable** if it has a model, and is unsatisfiable otherwise.

A model is **$A$-definable**, if each $p_i$ is definable by a formula $\bar{A}_i$ in $A$. 
Example Horn Encoding

```
int x = 1;
int y = 0;
while (*) {
    x = x + y;
    y = y + 1;
}
assert(x ≥ y);
```

```
\[\begin{align*}
\langle 1 \rangle & \quad p_0 . \\
\langle 2 \rangle & \quad p_1(x, y) \leftarrow \\
& \quad p_0, x = 1, y = 0 . \\
\langle 3 \rangle & \quad p_2(x, y) \leftarrow p_1(x, y) . \\
\langle 4 \rangle & \quad p_3(x, y) \leftarrow p_1(x, y) . \\
\langle 5 \rangle & \quad p_1(x', y') \leftarrow \\
& \quad p_2(x, y), \\
& \quad x' = x + y, \\
& \quad y' = y + 1 . \\
\langle 6 \rangle & \quad p_4 \leftarrow (x ≥ y), p_3(x, y) . \\
\langle 7 \rangle & \quad p_{err} \leftarrow (x < y), p_3(x, y) . \\
\langle 8 \rangle & \quad p_4 \leftarrow p_4 . \\
\langle 9 \rangle & \quad \bot \leftarrow p_{err} .
\end{align*}\]
```
Relationship between CHC and Verification

A program satisfies a property iff corresponding CHCs are satisfiable
- satisfiability-preserving transformations == safety preserving

Models for CHC correspond to verification certificates
- inductive invariants and procedure summaries

Unsatisfiability (or derivation of FALSE) corresponds to counterexample
- the resolution derivation (a path or a tree) is the counterexample

CAVEAT: In SeaHorn the terminology is reversed
- SAT means there exists a counterexample – a BMC at some depth is SAT
- UNSAT means the program is safe – BMC at all depths are UNSAT
FROM PROGRAMS TO CLAUSES
Hoare Triples

A Hoare triple \{\text{Pre}\} P \{\text{Post}\} is valid iff every terminating execution of \( P \) that starts in a state that satisfies \( \text{Pre} \) ends in a state that satisfies \( \text{Post} \).

Inductive Loop Invariant

\[
\begin{align*}
\text{Pre} \land \text{Inv} & \implies \{\text{Inv} \land \text{C}\} \text{Body} \{\text{Inv}\} \\
\text{Inv} \land \text{C} & \implies \text{Post}
\end{align*}
\]

\[
\{\text{Pre}\} \text{ while } \text{C} \text{ do } \text{Body} \{\text{Post}\}
\]

Function Application

\[
\begin{align*}
(\text{Pre} \land p=a) \land P & \implies \{P\} \text{Body}_F \{Q\} \\
(\text{Q} \land p,r=a,b) & \implies \text{Post}
\end{align*}
\]

\[
\{\text{Pre}\} b = F(a) \{\text{Post}\}
\]

Recursion

\[
\{\text{Pre}\} b = F(a) \{\text{Post}\} \land \{\text{Pre}\} \text{Body}_F \{\text{Post}\}
\]

\[
\{\text{Pre}\} b = F(a) \{\text{Post}\}
\]
Weakest Liberal Pre-Condition

Validity of Hoare triples is reduced to FOL validity by applying a predicate transformer

Dijkstra’s weakest liberal pre-condition calculus [Dijkstra’75]

\[ \text{wlp} (P, \text{Post}) \]

weakest pre-condition ensuring that executing \( P \) ends in \( \text{Post} \)

\[ \{\text{Pre}\} \ P \ \{\text{Post}\} \text{ is valid }, \ \text{Pre} ) \text{wlp} (P, \text{Post}) \]
A Simple Programming Language

Prog ::= def Main(x) { body_M }, ..., def P(x) { body_P }

body ::= stmt (; stmt)*

stmt ::= x = E | assert (E) | assume (E) | while E do S | y = P(E) | L:stmt | goto L (optional)

E ::= expression over program variables
Horn Clauses by Weakest Liberal Precondition

Prog ::= def Main(x) { body_M }, ..., def P(x) { body_P }

\[ \text{wlp } (x = E, Q) = \text{let } x = E \text{ in } Q \]
\[ \text{wlp } (\text{assert}(E), Q) = E \land Q \]
\[ \text{wlp } (\text{assume}(E), Q) = E \rightarrow Q \]
\[ \text{wlp } (\text{while } E \text{ do } S, Q) = I(w) \land \]
\[ 8w . ((I(w) \land E) \rightarrow \text{wlp } (S, I(w))) \land ((I(w) \land :E) \rightarrow Q)) \]
\[ \text{wlp } (y = P(E), Q) = p_{pre}(E) \land (8r. p(E, r) \rightarrow Q[r/y]) \]

\[ \text{ToHorn } (\text{def } P(x) \{ S \}) = \text{wlp } (x_0 = x; \text{assume}(p_{pre}(x)); S, p(x_0, \text{ret})) \]
\[ \text{ToHorn } (\text{Prog}) = \text{wlp } (\text{Main}(), \text{true}) \land 8\{P \land 2 \text{ Prog}\} \cdot \text{ToHorn } (P) \]
Example of a WLP Horn Encoding

\[
\{\text{Pre: } y \geq 0\}
\]
\[
x_0 = x;
\]
\[
y_0 = y;
\]
\[
\text{while } y > 0 \text{ do}
\]
\[
x = x + 1;
\]
\[
y = y - 1;
\]
\[
\{\text{Post: } x = x_0 + y_0\}
\]

\begin{align*}
\text{C1: } & I(x,y,x,y) \land y \geq 0. \\
\text{C2: } & I(x+1,y-1,x_0,y_0) \land I(x,y,x_0,y_0), \ y > 0. \\
\text{C3: } & \text{false} \land I(x,y,x_0,y_0), \ y \leq 0, \ x \neq x_0 + y_0
\end{align*}

\{y \geq 0\} \text{ P } \{x = x_{old} + y_{old}\} \text{ is true iff the query } C_3 \text{ is satisfiable}
Example Horn Encoding

int \ x = 1;
int \ y = 0;
while (*) {
    \ x = x + y;
    \ y = y + 1;
}
assert(\ x \geq \ y);

\begin{equation}
\begin{align*}
\langle 1 \rangle & \quad p_0. \\
\langle 2 \rangle & \quad p_1(x, y) \leftarrow p_0, x = 1, y = 0. \\
\langle 3 \rangle & \quad p_2(x, y) \leftarrow p_1(x, y). \\
\langle 4 \rangle & \quad p_3(x, y) \leftarrow p_1(x, y). \\
\langle 5 \rangle & \quad p_1(x', y') \leftarrow p_2(x, y), x' = x + y, y' = y + 1. \\
\langle 6 \rangle & \quad p_4 \leftarrow (x \geq y), p_3(x, y). \\
\langle 7 \rangle & \quad p_{err} \leftarrow (x < y), p_3(x, y). \\
\langle 8 \rangle & \quad p_4 \leftarrow p_4. \\
\langle 9 \rangle & \quad \bot \leftarrow p_{err}.
\end{align*}
\end{equation}
From CFG to Cut Point Graph

A Cut Point Graph hides (summarizes) fragments of a control flow graph by (summary) edges

Vertices (called, cut points) correspond to some basic blocks

An edge between cut-points $c$ and $d$ summarizes all finite (loop-free) executions from $c$ to $d$ that do not pass through any other cut-points
Cut Point Graph Example

CFG

CPG
Mixed Semantics

PROGRAM TRANSFORMATION
Deeply nested assertions
Deeply nested assertions

Counter-examples are long
Hard to determine (from main) what is relevant
Mixed Semantics

Stack-free program semantics combining:

• operational (or small-step) semantics
  – i.e., usual execution semantics
• natural (or big-step) semantics: function summary [Sharir-Pnueli 81]
  – \( (\frac{3}{4}, \frac{3}{4}') \) 2 \(|f|\) iff the execution of f on input state \( \frac{3}{4} \) terminates and results in state \( \frac{3}{4}' \)
• some execution steps are big, some are small

Non-deterministic executions of function calls

• update top activation record using function summary, or
• enter function body, forgetting history records (i.e., no return!)

Preserves reachability and non-termination

**Theorem:** Let \( K \) be the operational semantics, \( K^m \) the stack-free semantics, and \( L \) a program location. Then,

\[
K^2 \ EF \ (pc=L), \ K^m \ EF \ (pc=L) \quad \text{and} \quad K^2 \ EG \ (pc\neq L), \ K^m \ EG \ (pc\neq L)
\]
```python
def main()
1: int x = nd();
2: x = x+1;
3: while(x>=0)
4:   x=f(x);
5:   if(x<0)
6:     Error;
7:
8: END;

def f(int y):
9:   if(y>=10){
10:     y=y+1;
11:     y=f(y);
12:   } else if(y>0)
13:     y=y+1;
14:     y=y-1
15:
```

Summary of $f(y)$

$(1 \cdot x \cdot 9 \implies x' = x) \land (x \cdot 0 \implies x' = x - 1)$
Mixed Semantics as Program Transformation

```
main ()
  p1 (); p1 ();
  assert (c1);
  p1 ()
  p2 ();
  assert (c2);
  p2 ()
  assert (c3);
```

Mixed Semantics

```
main_new ()
  if (*) goto p1_entry;
  else p1_new ();
  if (*) goto p1_entry;
  else p1_new ();
  if (!c1) goto error;
  assume (false);

p1entry :
  if (*) goto p2_entry;
  else p2_new ();
  if (!c2) goto error;
  p2_entry :
  if (!c2) goto error;
  assume (false);

error : assert (false);
```

```
p1_new ()
  p2_new ();
  assume (c2);
  p2_new ()
  assume (c3);
```
Mixed Semantics: Summary

Every procedure is inlined at most once
• in the worst case, doubles the size of the program
• can be restricted to only inline functions that directly or indirectly call error() function

Easy to implement at compiler level
• create “failing” and “passing” versions of each function
• reduce “passing” functions to returning paths
• in main(), introduce new basic block bb.F for every failing function F(), and call failing.F in bb.F
• inline all failing calls
• replace every call to F to non-deterministic jump to bb.F or call to passing F

Increases context-sensitivity of context-insensitive analyses
• context of failing paths is explicit in main (because of inlining)
• enables / improves many traditional analyses
SOLVING CHC WITH SMT
Verification by Evolving Approximations

approx. 1

solver

approx. 2

solver

approx. 3

solver

Inductive Invariant

No

Safe?

No

Safe?

No

Safe?
Spacer: Solving CHC in Z3

Spacer: solver for SMT-constrained Horn Clauses
- stand-alone implementation in a fork of Z3
- http://bitbucket.org/spacer/code

Support for Non-Linear CHC
- model procedure summaries in inter-procedural verification conditions
- model assume-guarantee reasoning
- uses MBP to under-approximate models for finite unfoldings of predicates
- uses MAX-SAT to decide on an unfolding strategy

Supported SMT-Theories
- Best-effort support for arbitrary SMT-theories
  - data-structures, bit-vectors, non-linear arithmetic
- Full support for Linear arithmetic (rational and integer)
- Quantifier-free theory of arrays
  - only quantifier free models with limited applications of array equality
CRAB: Cornucopia of Abstractions

A library of abstract domains build on top of NASA Ikos (Inference Kernel for Open Static Analyzers)

A language-independent intermediate representation

Many abstract domains

• intervals (with congruences) (with uninterpreted functions)
• zones, dbms, octagons
• pointer analysis with offsets
• array analysis with smashing

Fixpoint iteration library

• precise interleaving between widening and narrowing
• extensible with thresholds

Efficient reusable data-structure

• simple API for integrating new abstract domains
RESULTS
SV-COMP 2015

4th Competition on Software Verification held (here!) at TACAS 2015

Goals

• Provide a snapshot of the state-of-the-art in software verification to the community.
• Increase the visibility and credits that tool developers receive.
• Establish a set of benchmarks for software verification in the community.

Participants:

• Over 22 participants, including most popular Software Model Checkers and Bounded Model Checkers

Benchmarks:

• C programs with error location (programs include pointers, structures, etc.)
• Over 6,000 files, each 2K – 100K LOC
• Linux Device Drivers, Product Lines, Regressions/Tricky examples
• http://sv-comp.sosy-lab.org/2015/benchmarks.php
Results for DeviceDriver category
Detecting Buffer Overflow in Auto-pilot software

Show absence of Buffer Overflows in
- paparazzi and mnav autopilots

Automatically instrument buffer accesses with runtime checks
Use SeaHorn to validate that run-time checks never fail
- somewhat slower than pure abstract interpretation
- much more precise!

LLVM Pass to insert BO checks
Conclusion

SeaHorn (http://seahorn.github.io)
- a state-of-the-art Software Model Checker
- LLVM-based front-end
- CHC-based verification engine
- a framework for research in logic-based verification

The future
- making SeaHorn useful to users of verification technology
  - counterexamples, build integration, property specification, proofs, etc.
- targeting many existing CHC engines
  - specialize encoding and transformations to specific engines
  - communicate results between engines
- richer properties
  - termination, liveness, synthesis
Available postdoctoral positions

What: development and application of SeaHorn

Where: CMU/NASA Silicon Valley Campus

Contact:
Temegshon Kahasai
temesghen.kahasai@nasa.gov
Arie Gurfinkel arie@cmu.edu
Programs, Cexs, Invariants

A program \( P = (V, \text{Init}, \frac{1}{2}, \text{Bad}) \)

- Notation: \( F(X) = \exists u . (X \not\in \frac{1}{2}) \subset \text{Init} \)

\( P \) is UNSAFE if and only if there exists a number \( N \) s.t.

\[
\text{Init}(v_0) \land \left( \bigwedge_{i=0}^{N-1} \rho(v_i, v_{i+1}) \right) \land \text{Bad}(v_N) \not\Rightarrow \bot
\]

\( P \) is SAFE if and only if there exists a safe inductive invariant \( \text{Inv} \) s.t.

\[
\begin{align*}
\text{Init}(u) & \Rightarrow \text{Inv}(u) \\
\text{Inv}(u) \land \rho(u, v) & \Rightarrow \text{Inv}(v) \\
\text{Inv}(u) & \Rightarrow \neg\text{Bad}(u)
\end{align*}
\]
IC3/PDR Algorithm Overview

Input: Safety problem $\langle \text{Init}(X), \text{Tr}(X, X'), \text{Bad}(X) \rangle$

$F_0 \leftarrow \text{Init} ; N \leftarrow 0$ repeat

$\textbf{G} \leftarrow \text{PdrMkSafe}([F_0, \ldots, F_N], \text{Bad})$

\textbf{if} $\textbf{G} = []$ then return $\text{Reachable}$;

$\forall 0 \leq i \leq N \cdot F_i \leftarrow G[i]$

$F_0, \ldots, F_N \leftarrow \text{PdrPush}([F_0, \ldots, F_N])$

\textbf{if} $\exists 0 \leq i < N \cdot F_i = F_{i+1}$ then return $\text{Unreachable}$;

$N \leftarrow N + 1 ; F_N \leftarrow \emptyset$

until $\infty$;
IC3/PDR in Pictures
IC3/PDR in Pictures

Cex Queue

PdrMkSafe

Trace

Frame $R_0$

Frame $R_1$

lemma

cex

Veriﬁcation with SeaHorn
Gurfinkel, 2015
© 2015 Carnegie Mellon University
IC3/PDR in Pictures

Inductive
Verification with SeaHorn
Gurfinkel, 2015
© 2015 Carnegie Mellon University

IC3/PDR in Pictures

PDR Invariants

\[ R_i \rightarrow : \text{Bad} \quad \text{Init} \rightarrow R_i \]
\[ R_i \rightarrow R_{i+1} \quad R_i \mathcal{A} \ 1/2 \rightarrow R_{i+1} \]