Counterexample-guided Approach to Finding Numerical Invariants

ThanhVu (Vu) Nguyen*,
Timos Antonopoulous†, Andrew Ruef‡, Michael Hicks‡

*University of Nebraska, †Yale University, ‡University of Maryland

FSE 2017
Invariants are asserted properties, such as relations among variables that always hold at certain locations in a program

- Assertions
- Pre/Post conditions
- Loop invariants
Introduction

*Invariants are asserted properties, such as relations among variables that always hold at certain locations in a program*

- Assertions
- Pre/Post conditions
- Loop invariants

Techniques for automatic invariant generation

- *Static*: examine program code, compute sound results, but can be expensive and limited to simple invariants
- *Dynamic*: analyze exec traces, produce expressive invariants, but unsound
Invariants are asserted properties, such as relations among variables that always hold at certain locations in a program

- Assertions
- Pre/Post conditions
- Loop invariants

Techniques for automatic invariant generation

- Static: examine program code, compute sound results, but can be expensive and limited to simple invariants
- Dynamic: analyze exec traces, produce expressive invariants, but unsound

Numerical invariants, e.g., relations among numerical variables

- E.g., $x = 2y + 3, 0 \leq idx \leq |arr| - 1, x \leq y^2, x = qy + r$
- Nonlinear polynomial invariants: $x \leq y^2, x = qy + r, \ldots$
Invariants can help understanding programs

```c
int cohendiv(int x, int y) {
    assert(x>0 && y>0);
    int q=0; int r=x;
    while(r ≥ y){
        int a=1;
        int b=y;
        while[L1](r ≥ 2*b){
            a = 2*a;
            b = 2*b;
        }
        r=r-b;
        q=q+a;
    }
    [L2]
    return q;
}
```

What does this program do? What properties hold at \textbf{L1} and \textbf{L2}?

- Loop invariants at \textbf{L1}:
  - \( x = qy + r \)
  - \( b = ya \)
  - \( y \leq b \)
  - \( b \leq r \)
  - \( r \leq x \)
  - \( a \leq b + y \)

- Postconditions at \textbf{L2}:
  - \( x = qy + r \)
  - \( 1 \leq q + r \)
  - \( r \leq y - 1 \)
  - \( 0 \leq r \)
  - \( r \leq x \)

Describe the semantic the program (e.g., \( x = qy + r \) for integer division) and reveal useful information (e.g., remainder \( r \) is non-negative).
Invariants can help understanding programs

```c
int cohendiv(int x, int y){
    assert(x>0 && y>0);
    int q=0; int r=x;
    while(r ≥ y){
        int a=1;
        int b=y;
        while[L1](r ≥ 2*b){
            a = 2*a;
            b = 2*b;
        }
        r=r-b;
        q=q+a;
    }
    [L2]
    return q;
}
```

What does this program do? What properties hold at L1 and L2?

- **loop invariants at L1:**
  
  \[ x = qy + r \quad b = ya \]
  
  \[ y \leq b \quad b \leq r \]
  
  \[ r \leq x \quad a \leq b \]
  
  \[ 2 \leq a + y \]

- **postconditions at L2:**
  
  \[ x = qy + r \]
  
  \[ 1 \leq q + r \quad r \leq y - 1 \]
  
  \[ 0 \leq r \quad r \leq x \]
int cohendiv(int x, int y){
    assert(x>0 && y>0);
    int q=0; int r=x;
    while(r ≥ y){
        int a=1;
        int b=y;
        while[L1](r ≥ 2*b){
            a = 2*a;
            b = 2*b;
        }
        r=r-b;
        q=q+a;
    }
    [L2]
    return q;
}

What does this program do? What properties hold at L1 and L2?

- loop invariants at L1:
  - x = qy + r
  - b = ya
  - y ≤ b
  - b ≤ r
  - r ≤ x
  - a ≤ b
  - 2 ≤ a + y

- postconditions at L2:
  - x = qy + r
  - 1 ≤ q + r
  - r ≤ y - 1
  - 0 ≤ r
  - r ≤ x

Describe the semantic the program (e.g., \( x = qy + r \) for integer division) and reveal useful information (e.g., remainder \( r \) is non-negative)
void triple(int M, int N, int P){
    assert (0 <= M);
    assert (0 <= N);
    assert (0 <= P);
    int i = 0, j = 0, k = 0;
    int t = 0;
    while(i < N){
        j = 0; t++;
        while(j < M){
            j++; k = i; t++;
            while (k < P){
                k++; t++;
            }
            i = k;
        }
        i++;
    }
    [L]
}
void triple(int M, int N, int P){
    assert (0 <= M);
    assert (0 <= N);
    assert (0 <= P);
    int i = 0, j = 0, k = 0;
    int t = 0;
    while(i < N){
        j = 0; t++;
        while(j < M){
            j++; k = i; t++;
            while (k < P){
                k++; t++;
            }
            i = k;
        }
        i++;
    }
    [L]
}
Invariants can help verify programs

```c
void f(int u1, int u2) {
    assert(u1 > 0 && u2 > 0);
    int a = 1, b = 1, c = 2, d = 2;
    int x = 3, y = 3;
    int i1 = 0, i2 = 0;
    while (i1 < u1) {
        i1++;
        x = a + c; y = b + d;
        if ((x + y) % 2 == 0) {
            a++; d++;
        } else { a--;}
    } else { a--;}
    i2 = 0;
    while (i2 < u2 ) {
        i2++; c--; b--;
    }
}

[L]
assert(a + c == b + d);
}

void g(int n, int u1) {
    assert(u1 > 0);
    int x = 0;
    int m = 0;
    while (x < n) {
        if (u1) {
            m = x;
        }
        x = x + 1;
    }
    [L]
    if (n > 0){
        assert(0 <= m && m < n);
    }
}
```
void f(int u1, int u2) {
    assert(u1 > 0 && u2 > 0);
    int a = 1, b = 1, c = 2, d = 2;
    int x = 3, y = 3;
    int i1 = 0, i2 = 0;
    while (i1 < u1) {
        i1++;
        x = a + c; y = b + d;
        if ((x + y) % 2 == 0) {
            a++; d++;
        } else { a--;}
    }
    i2 = 0;
    while (i2 < u2) {
        i2++;
        c--; b--;
    }
    assert(a + c == b + d);
}

void g(int n, int u1) {
    assert(u1 > 0);
    int x = 0;
    int m = 0;
    while (x < n) {
        if (u1) {
            m = x;
        }
        x = x + 1;
    }
    if (n > 0){
        assert(0 <= m && m < n);
    }
}

Assertions hold if matched or implied by discovered invariants at L
**NumInv: a CEGIR approach to numerical invariants**

- Focus on polynomial invariants over numerical variables
- Use CounterExample-Guided Invariant Generation (CEGIR) approach
  - Dynamic Inference: use DIG’s algorithms to infer *nonlinear equalities* and *linear inequalities* from traces
  - Static Checking: use KLEE to check candidate invariants and generate counterexample inputs
Example: Dynamic Inference using DIG

```c
int cohendiv(int x, int y){
    assert(x>0 ; y>0);
    int q=0; int r=x;
    while(r >= y){
        int a=1; int b=y;
        while[L1](r >= 2*b){
            a = 2*a; b = 2*b;
        }
        r=r-b; q=q+a;
    }
    return q;
}
```

Traces:

<table>
<thead>
<tr>
<th>x</th>
<th>y</th>
<th>a</th>
<th>b</th>
<th>q</th>
<th>r</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>15</td>
</tr>
<tr>
<td>15</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>15</td>
</tr>
<tr>
<td>15</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>4</td>
</tr>
</tbody>
</table>

Loop invariants at L1:

**equations**:

- \( x = qy + r \)
- \( b = ya \)

**inequalities**:

- \( 2 \leq a + y \)
- \( a \leq b \)
- \( b \leq r \)
- \( r \leq x \)
int cohendiv(int x, int y){
    assert(x>0 ; y>0);
    int q=0; int r=x;
    while(r >= y){
        int a=1; int b=y;
        while[r >= 2*b]{
            a = 2*a; b = 2*b;
        }
        r=r-b; q=q+a;
    }
    return q;
}

Traces:

<table>
<thead>
<tr>
<th>x</th>
<th>y</th>
<th>a</th>
<th>b</th>
<th>q</th>
<th>r</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>15</td>
</tr>
<tr>
<td>15</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>15</td>
</tr>
<tr>
<td>15</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Loop invariants at L1:
equations: x = qy + r
inequalities: 2 ≤ a + y a ≤ b y ≤ b b ≤ r r ≤ x

7
int cohendiv(int x, int y){
    assert(x>0 ; y>0);
    int q=0; int r=x;
    while(r >= y){
        int a=1; int b=y;
        while([L1](r >= 2*b){
            a = 2*a; b = 2*b;
        }r=r-b; q=q+a;
    }
    return q;
}

Traces:

<table>
<thead>
<tr>
<th>x</th>
<th>y</th>
<th>a</th>
<th>b</th>
<th>q</th>
<th>r</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>15</td>
</tr>
<tr>
<td>15</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>15</td>
</tr>
<tr>
<td>15</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Loop invariants at L1:

* equations:  \[ x = qy + r \quad b = ya \]
* inequalities:  \[ 2 \leq a + y \quad a \leq b \quad y \leq b \]
\[ b \leq r \quad r \leq x \]
Infer Nonlinear Equations using Equation Solver

Terms and degrees

\[ V = \{ r, y, a \}; \quad \text{deg} = 2 \]

\[ T = \{ 1, r, y, a, ry, ra, ya, r^2, y^2, a^2 \} \]

Nonlinear equation template

\[ c_1 + c_2 r + c_3 y + c_4 a + c_5 ry + c_6 ra + c_7 ya + c_8 r^2 + c_9 y^2 + c_{10} a^2 = 0 \]

System of linear equations

\[ V = \{ x, y, a, b, q, r \}; \quad \text{deg} = 2 \rightarrow x = qy + r, \quad b = ya \]

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>15</td>
</tr>
<tr>
<td>15</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>15</td>
</tr>
<tr>
<td>15</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>4</td>
</tr>
</tbody>
</table>
Infer Nonlinear Equations using Equation Solver

- Terms and degrees

\[ V = \{ r, y, a \}; \text{ deg } = 2 \]

\[ T = \{ 1, r, y, a, ry, ra, ya, r^2, y^2, a^2 \} \]

<table>
<thead>
<tr>
<th>x</th>
<th>y</th>
<th>a</th>
<th>b</th>
<th>q</th>
<th>r</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>15</td>
</tr>
<tr>
<td>15</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>15</td>
</tr>
<tr>
<td>15</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>4</td>
</tr>
</tbody>
</table>
**Infer Nonlinear Equations using Equation Solver**

- **Terms and degrees**
  \[ V = \{ r, y, a \}; \quad \text{deg} = 2 \]
  \[ \downarrow \]
  \[ T = \{ 1, r, y, a, ry, ra, ya, r^2, y^2, a^2 \} \]

- **Nonlinear equation template**
  \[ c_1 + c_2 r + c_3 y + c_4 a + c_5 ry + c_6 ra + c_7 ya + c_8 r^2 + c_9 y^2 + c_{10} a^2 = 0 \]

<table>
<thead>
<tr>
<th></th>
<th>x</th>
<th>y</th>
<th>a</th>
<th>b</th>
<th>q</th>
<th>r</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>2</td>
<td></td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>15</td>
</tr>
<tr>
<td>15</td>
<td>2</td>
<td></td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>15</td>
</tr>
<tr>
<td>15</td>
<td>2</td>
<td></td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td></td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td></td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>4</td>
</tr>
</tbody>
</table>
Infer Nonlinear Equations using Equation Solver

- Terms and degrees

\[ V = \{r, y, a\}; \quad \text{deg} = 2 \]

\[ T = \{1, r, y, a, ry, ra, ya, r^2, y^2, a^2\} \]

- Nonlinear equation template

\[ c_1 + c_2 r + c_3 y + c_4 a + c_5 ry + c_6 ra + c_7 ya + c_8 r^2 + c_9 y^2 + c_{10} a^2 = 0 \]

- System of linear equations

\begin{align*}
\text{trace 1} & \quad \rightarrow \quad \{r = 15, y = 2, a = 1\} \\
\text{eq 1} & \quad \rightarrow \quad c_1 + 15c_2 + 2c_3 + c_4 + 30c_5 + 15c_6 + 2c_7 + 225c_8 + 4c_9 + c_{10} = 0 \\
\vdots
\end{align*}
Infer Nonlinear Equations using Equation Solver

- Terms and degrees

\[ V = \{ r, y, a \}; \text{ deg} = 2 \]

\[ T = \{ 1, r, y, a, ry, ra, ya, r^2, y^2, a^2 \} \]

- Nonlinear equation template

\[ c_1 + c_2 r + c_3 y + c_4 a + c_5 ry + c_6 ra + c_7 ya + c_8 r^2 + c_9 y^2 + c_{10} a^2 = 0 \]

- System of linear equations

<table>
<thead>
<tr>
<th>x</th>
<th>y</th>
<th>a</th>
<th>b</th>
<th>q</th>
<th>r</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>15</td>
</tr>
<tr>
<td>15</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>15</td>
</tr>
<tr>
<td>15</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>4</td>
</tr>
</tbody>
</table>

- Solve for coefficients \( c_i \)

\[ V = \{ x, y, a, b, q, r \}; \text{ deg} = 2 \quad \rightarrow \quad x = qy + r, \ b = ya \]
Static Checking

- **Goal:** prove/refute candidate invariants using program code
- **Approach:** reduce invariant checking to reachability

\[ L' \]
\[ \text{is } x = qy + r \text{ valid?} \]
\[ \Rightarrow \]
\[ \text{if } !(x == qy + r) \{
   L' \}
\]
\[ \text{x = qy + r is invalid} \]
\[ \text{abort();} \]
\[ \text{x = qy + r is valid} \]

\[ L' \text{ reachable} \Rightarrow \text{inv is spurious (inputs reaching L' represent cex's)} \]
\[ L' \text{ not reachable (within a time bound)} \Rightarrow \text{NumInv accepts the invariant} \]

Use the symbolic execution tool KLEE to check reachability

Unsound: KLEE can timeout, but in practice is very effective in refuting bad invariants and finding cex's

Can use other test-input generation tools or verifiers instead of KLEE
Static Checking

- **Goal**: prove/refute candidate invariants using program code
- **Approach**: reduce invariant checking to reachability
  - Transform program and invariant into another program consist of a special location $L'$

```
... [L] //is x=qy+r valid?  =>  ... if (!(x==qy+r)) {
    [L'] //x=qy+r is invalid
    abort();
} //x=qy+r is valid
...
```
Static Checking

- **Goal**: prove/refute candidate invariants using program code
- **Approach**: reduce invariant checking to reachability
  - Transform program and invariant into another program consist of a special location \( L' \)
    
    ```
    ...  
    if (!(x==qy+r)){  
      [L']  //x=qy+r is invalid  
      abort();  
    }  
    //x=qy+r is valid  
    ...
    ```

  - \( L' \) reachable \( \Rightarrow \) inv is spurious (inputs reaching \( L' \) represent cex’s)
  - \( L' \) not reachable (within a time bound) \( \Rightarrow \) NumInv *accepts* the invariant

Use the symbolic execution tool KLEE to check reachability

Unsound: KLEE can timeout, but in practice is very effective in refuting bad invariants and finding cex’s

Can use other test-input generation tools or verifiers instead of KLEE
Static Checking

- **Goal**: prove/refute candidate invariants using program code
- **Approach**: reduce invariant checking to reachability
  - Transform program and invariant into another program consist of a special location $L'$

```plaintext
... [L] //is x=qy+r valid?  ⇒  abort();
... [L'] //x=qy+r is invalid
  if (!x==qy+r) {
    [L'] //x=qy+r is invalid
  }
  //x=qy+r is valid
  ...
```

- $L'$ reachable $⇒$ inv is spurious (inputs reaching $L'$ represent cex’s)
- $L'$ not reachable (within a time bound) $⇒$ NumInv accepts the invariant

- Use the symbolic execution tool **KLEE** to check reachability
  - **Unsound**: KLEE can timeout, but in practice is **very effective** in refuting bad invariants and finding cex’s
  - Can use other test-input generation tools or verifiers instead of KLEE
Evaluation

Setup
- NumInv is implemented in SAGE/Python (with Z3 backend solver)
- Test machine: 10-core 2.4GHZ CPU, 128GB Ram, Linux OS

Benchmark
- Program Understanding: NLA testsuite, 27 programs with nonlinear invariants
- Complexity Analysis: 19 programs collected from static complexity analysis work
- Program Verification: HOLA benchmark, 46 programs with assertions, compare against PIE
int cohendiv(int x, int y){
    assert(x>0 && y>0);
    int q=0; int r=x;
    while(r ≥ y){
        int a=1;
        int b=y;
        while [L1](r ≥ 2*b){
            a = 2*a;
            b = 2*b;
        }
        r=r-b;
        q=q+a;
    }
    [L2]
    return q;
}
int cohendiv(int x, int y){
    assert(x>0 && y>0);
    int q=0; int r=x;
    while(r ≥ y){
        int a=1;
        int b=y;
        while[L1](r ≥ 2*b){
            a = 2*a;
            b = 2*b;
        }
        r=r-b;
        q=q+a;
    }
    [L2]
    return q;
}

What does this program do? What properties hold at L1 and L2?

- **loop invariants at L1:**

\[
\begin{align*}
    x &= qy + r \quad b = ya \\
    y &\leq b \quad b \leq r \\
    r &\leq x \quad a \leq b \\
    2 &\leq a + y
\end{align*}
\]

- **postconditions at L2:**

\[
\begin{align*}
    x &= qy + r \\
    1 &\leq q + r \quad r \leq y - 1 \\
    0 &\leq r \quad r \leq x
\end{align*}
\]

Indicate the exact semantic of integer division and reveal other useful correctness information (e.g., remainder is non-negative).
Example: Program Understanding

```c
int cohendiv(int x, int y){
    assert(x>0 && y>0);
    int q=0; int r=x;
    while(r ≥ y){
        int a=1;
        int b=y;
        while[L1](r ≥ 2*b){
            a = 2*a;
            b = 2*b;
        }
        r=r-b;
        q=q+a;
    }
    [L2]
    return q;
}
```

What does this program do? What properties hold at L1 and L2?

- **loop invariants at L1:**
  - \( x = qy + r \)
  - \( b = ya \)
  - \( y \leq b \)
  - \( b \leq r \)
  - \( r \leq x \)
  - \( a \leq b \)
  - \( 2 \leq a + y \)

- **postconditions at L2:**
  - \( x = qy + r \)
  - \( 1 \leq q + r \)
  - \( r \leq y - 1 \)
  - \( 0 \leq r \)
  - \( r \leq x \)

Indicate the exact semantic of integer division and reveal other useful correctness information (e.g., remainder is non-negative)
Results: Program Understanding

<table>
<thead>
<tr>
<th>Prog</th>
<th>Locs</th>
<th>Invs</th>
<th>Time (s)</th>
<th>Correct</th>
</tr>
</thead>
<tbody>
<tr>
<td>cohendiv</td>
<td>2</td>
<td>11</td>
<td>24.5</td>
<td>✓</td>
</tr>
<tr>
<td>divbin</td>
<td>2</td>
<td>12</td>
<td>116.8</td>
<td>✓</td>
</tr>
<tr>
<td>manna</td>
<td>1</td>
<td>5</td>
<td>30.8</td>
<td>✓</td>
</tr>
<tr>
<td>hard</td>
<td>2</td>
<td>13</td>
<td>71.4</td>
<td>✓</td>
</tr>
<tr>
<td>sqrt1</td>
<td>1</td>
<td>5</td>
<td>19.3</td>
<td>✓</td>
</tr>
<tr>
<td>dijkstra</td>
<td>2</td>
<td>14</td>
<td>89.3</td>
<td>✓</td>
</tr>
<tr>
<td>freire1</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>freire2</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>cohencu</td>
<td>1</td>
<td>5</td>
<td>22.5</td>
<td>✓</td>
</tr>
<tr>
<td>egcd1</td>
<td>1</td>
<td>9</td>
<td>284.5</td>
<td>✓</td>
</tr>
<tr>
<td>egcd2</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>egcd3</td>
<td>3</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>prodbin</td>
<td>1</td>
<td>7</td>
<td>45.1</td>
<td>✓</td>
</tr>
<tr>
<td>prod4br</td>
<td>1</td>
<td>11</td>
<td>87.3</td>
<td>✓</td>
</tr>
<tr>
<td>knuth</td>
<td>1</td>
<td>9</td>
<td>84.6</td>
<td>✓</td>
</tr>
<tr>
<td>fermat1</td>
<td>3</td>
<td>26</td>
<td>185.3</td>
<td>✓</td>
</tr>
<tr>
<td>fermat2</td>
<td>1</td>
<td>8</td>
<td>101.8</td>
<td>✓</td>
</tr>
<tr>
<td>lcm1</td>
<td>3</td>
<td>22</td>
<td>175.2</td>
<td>✓</td>
</tr>
<tr>
<td>lcm2</td>
<td>1</td>
<td>7</td>
<td>163.8</td>
<td>✓</td>
</tr>
<tr>
<td>geo1</td>
<td>1</td>
<td>7</td>
<td>24.4</td>
<td>✓</td>
</tr>
<tr>
<td>geo2</td>
<td>1</td>
<td>9</td>
<td>24.3</td>
<td>✓</td>
</tr>
<tr>
<td>geo3</td>
<td>1</td>
<td>7</td>
<td>32.3</td>
<td>✓</td>
</tr>
<tr>
<td>ps2</td>
<td>1</td>
<td>3</td>
<td>17.0</td>
<td>✓</td>
</tr>
<tr>
<td>ps3</td>
<td>1</td>
<td>4</td>
<td>17.8</td>
<td>✓</td>
</tr>
<tr>
<td>ps4</td>
<td>1</td>
<td>4</td>
<td>18.5</td>
<td>✓</td>
</tr>
<tr>
<td>ps5</td>
<td>1</td>
<td>4</td>
<td>19.3</td>
<td>✓</td>
</tr>
<tr>
<td>ps6</td>
<td>1</td>
<td>3</td>
<td>21.0</td>
<td>✓</td>
</tr>
</tbody>
</table>

Experiment

- **NLA suite**: 27 programs
- Require nonlinear invariants
- Use documented invariants (loop invariants and postconds) as ground truths
- **Goal**: obtain invariants and compare to ground truths
Results: Program Understanding

<table>
<thead>
<tr>
<th>Prog</th>
<th>Locs</th>
<th>Invs</th>
<th>Time (s)</th>
<th>Correct</th>
</tr>
</thead>
<tbody>
<tr>
<td>cohendiv</td>
<td>2</td>
<td>11</td>
<td>24.5</td>
<td>✓</td>
</tr>
<tr>
<td>divbin</td>
<td>2</td>
<td>12</td>
<td>116.8</td>
<td>✓</td>
</tr>
<tr>
<td>manna</td>
<td>1</td>
<td>5</td>
<td>30.8</td>
<td>✓</td>
</tr>
<tr>
<td>hard</td>
<td>2</td>
<td>13</td>
<td>71.4</td>
<td>✓</td>
</tr>
<tr>
<td>sqrt1</td>
<td>1</td>
<td>5</td>
<td>19.3</td>
<td>✓</td>
</tr>
<tr>
<td>dijkstra</td>
<td>2</td>
<td>14</td>
<td>89.3</td>
<td>✓</td>
</tr>
<tr>
<td>freire1</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>freire2</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>cohencu</td>
<td>1</td>
<td>5</td>
<td>22.5</td>
<td>✓</td>
</tr>
<tr>
<td>egcd1</td>
<td>1</td>
<td>9</td>
<td>284.5</td>
<td>✓</td>
</tr>
<tr>
<td>egcd2</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>egcd3</td>
<td>3</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>prodbin</td>
<td>1</td>
<td>7</td>
<td>45.1</td>
<td>✓</td>
</tr>
<tr>
<td>prod4br</td>
<td>1</td>
<td>11</td>
<td>87.3</td>
<td>✓</td>
</tr>
<tr>
<td>knuth</td>
<td>1</td>
<td>9</td>
<td>84.6</td>
<td>✓</td>
</tr>
<tr>
<td>fermat1</td>
<td>3</td>
<td>26</td>
<td>185.3</td>
<td>✓</td>
</tr>
<tr>
<td>fermat2</td>
<td>1</td>
<td>8</td>
<td>101.8</td>
<td>✓</td>
</tr>
<tr>
<td>lcm1</td>
<td>3</td>
<td>22</td>
<td>175.2</td>
<td>✓</td>
</tr>
<tr>
<td>lcm2</td>
<td>1</td>
<td>7</td>
<td>163.8</td>
<td>✓</td>
</tr>
<tr>
<td>geo1</td>
<td>1</td>
<td>7</td>
<td>24.4</td>
<td>✓</td>
</tr>
<tr>
<td>geo2</td>
<td>1</td>
<td>9</td>
<td>24.3</td>
<td>✓</td>
</tr>
<tr>
<td>geo3</td>
<td>1</td>
<td>7</td>
<td>32.3</td>
<td>✓</td>
</tr>
<tr>
<td>ps2</td>
<td>1</td>
<td>3</td>
<td>17.0</td>
<td>✓</td>
</tr>
<tr>
<td>ps3</td>
<td>1</td>
<td>4</td>
<td>17.8</td>
<td>✓</td>
</tr>
<tr>
<td>ps4</td>
<td>1</td>
<td>4</td>
<td>18.5</td>
<td>✓</td>
</tr>
<tr>
<td>ps5</td>
<td>1</td>
<td>4</td>
<td>19.3</td>
<td>✓</td>
</tr>
<tr>
<td>ps6</td>
<td>1</td>
<td>3</td>
<td>21.0</td>
<td>✓</td>
</tr>
</tbody>
</table>

Experiment

- **NLA suite**: 27 programs
- Require nonlinear invariants
- Use documented invariants (loop invariants and postconds) as ground truths
- **Goal**: obtain invariants and compare to ground truths

**Results**: NumInv found correct invariants in 23/27 progs

- Most results equiv to or stronger than (imply) ground truths
- Several unexpected and undocumented invariants
- Some invariants reveal “how” program works in details
Example: Complexity Analysis

void triple(int M, int N, int P){
    assert (0 <= M);
    assert (0 <= N);
    assert (0 <= P);
    int i = 0, j = 0, k = 0;
    int t = 0;
    while(i < N){
        j = 0; t++;
        while(j < M){
            j++; k = i; t++;
            while (k < P){
                k++; t++;
            }
        i = k;
    }
    i++;}
} [L]

Complexity of this program?

- Existing result: $t = O(N + NM + P)$

Nonlinear invariants can represent disjunctive properties capturing different complexity bounds.
Example: Complexity Analysis

```c
void triple(int M, int N, int P){
    assert (0 <= M);
    assert (0 <= N);
    assert (0 <= P);
    int i = 0, j = 0, k = 0;
    int t = 0;
    while(i < N){
        j = 0; t++;
        while(j < M){
            j++; k = i; t++;
            while (k < P){
                k++; t++;
            }
            i = k;
        }
        i++;
    }
    [L]
}
```

Complexity of this program?

- Existing result: \( t = O(N + NM + P) \)
- NumInv found a very unexpected inv:

\[
P^2Mt + PM^2t - PMNt - M^2Nt
- PMt^2 + MNt^2 + PMt - PNd - 2MNd
+ Pt^2 + Mt^2 + Nt^2 - t^3 - Nt + t^2 = 0
\]

Nonlinear invariants can represent disjunctive properties.
Example: Complexity Analysis

void triple(int M, int N, int P) {
    assert (0 <= M);
    assert (0 <= N);
    assert (0 <= P);
    int i = 0, j = 0, k = 0;
    int t = 0;
    while (i < N) {
        j = 0; t++;
        while (j < M) {
            j++; k = i; t++;
            while (k < P) {
                k++; t++;
            }
            i = k;
        }
        i++;
    }
}

Complexity of this program?

- Existing result: $t = O(N + NM + P)$
- NumInv found a very unexpected inv:

$$
P^2 Mt + PM^2 t - PMNt - M^2 N t \\
- PMt^2 + MNt^2 + PMt - P N t - 2MNt \\
+ Pt^2 + Mt^2 + N t^2 - t^3 - N t + t^2 = 0
$$

- Solve for $t$ yields the most precise, unpublished bound:

$$
t = 0 \quad \text{when } N = 0, \\
t = P + M + 1 \quad \text{when } N \leq P, \\
t = N - M(P - N) \quad \text{when } N > P
$$

- Nonlinear invariants can represent disjunctive properties capturing different complexity bounds
Results: Complexity Analysis

<table>
<thead>
<tr>
<th>Prog</th>
<th>Invs</th>
<th>Time (s)</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>cav09_fig1a</td>
<td>1</td>
<td>14.3</td>
<td>✓</td>
</tr>
<tr>
<td>cav09_fig1d</td>
<td>1</td>
<td>14.2</td>
<td>✓</td>
</tr>
<tr>
<td>cav09_fig2d</td>
<td>3</td>
<td>36.0</td>
<td>✓</td>
</tr>
<tr>
<td>cav09_fig3a</td>
<td>3</td>
<td>14.2</td>
<td>✓</td>
</tr>
<tr>
<td>cav09_fig5b</td>
<td>5</td>
<td>46.8</td>
<td>✓</td>
</tr>
<tr>
<td>pldi09_ex6</td>
<td>7</td>
<td>54.1</td>
<td>✓</td>
</tr>
<tr>
<td>pldi09_fig2 (triple)</td>
<td>6</td>
<td>93.5</td>
<td>✓✓</td>
</tr>
<tr>
<td>pldi09_fig4_1</td>
<td>3</td>
<td>44.2</td>
<td>✓</td>
</tr>
<tr>
<td>pldi09_fig4_2</td>
<td>5</td>
<td>43.7</td>
<td>✓</td>
</tr>
<tr>
<td>pldi09_fig4_3</td>
<td>3</td>
<td>37.5</td>
<td>✓</td>
</tr>
<tr>
<td>pldi09_fig4_4</td>
<td>4</td>
<td>56.6</td>
<td>-</td>
</tr>
<tr>
<td>pldi09_fig4_5</td>
<td>3</td>
<td>31.6</td>
<td>✓</td>
</tr>
<tr>
<td>popl09_fig2_1</td>
<td>2</td>
<td>211.7</td>
<td>✓✓</td>
</tr>
<tr>
<td>popl09_fig2_2</td>
<td>2</td>
<td>65.1</td>
<td>✓✓</td>
</tr>
<tr>
<td>popl09_fig3_4</td>
<td>4</td>
<td>54.7</td>
<td>✓</td>
</tr>
<tr>
<td>popl09_fig4_1</td>
<td>2</td>
<td>42.7</td>
<td>✓</td>
</tr>
<tr>
<td>popl09_fig4_2</td>
<td>2</td>
<td>158.3</td>
<td>✓✓</td>
</tr>
<tr>
<td>popl09_fig4_3</td>
<td>5</td>
<td>39.2</td>
<td>✓</td>
</tr>
<tr>
<td>popl09_fig4_4</td>
<td>3</td>
<td>34.2</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Experiment**

- 19 progs from static complexity work
- Obtain postconds representing complexity
- **Goal**: compare against results from prev work
**Results: Complexity Analysis**

<table>
<thead>
<tr>
<th>Prog</th>
<th>Invs</th>
<th>Time (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>cav09_fig1a</td>
<td>1</td>
<td>14.3</td>
</tr>
<tr>
<td>cav09_fig1d</td>
<td>1</td>
<td>14.2</td>
</tr>
<tr>
<td>cav09_fig2d</td>
<td>3</td>
<td>36.0</td>
</tr>
<tr>
<td>cav09_fig3a</td>
<td>3</td>
<td>14.2</td>
</tr>
<tr>
<td>cav09_fig5b</td>
<td>5</td>
<td>46.8</td>
</tr>
<tr>
<td>pldi09_ex6</td>
<td>7</td>
<td>54.1</td>
</tr>
<tr>
<td>pldi09_fig2 (triple)</td>
<td>6</td>
<td>93.5</td>
</tr>
<tr>
<td>pldi09_fig4_1</td>
<td>3</td>
<td>44.2</td>
</tr>
<tr>
<td>pldi09_fig4_2</td>
<td>5</td>
<td>43.7</td>
</tr>
<tr>
<td>pldi09_fig4_3</td>
<td>3</td>
<td>37.5</td>
</tr>
<tr>
<td>pldi09_fig4_4</td>
<td>4</td>
<td>56.6</td>
</tr>
<tr>
<td>pldi09_fig4_5</td>
<td>3</td>
<td>31.6</td>
</tr>
<tr>
<td>popl09_fig2_1</td>
<td>2</td>
<td>211.7</td>
</tr>
<tr>
<td>popl09_fig2_2</td>
<td>2</td>
<td>65.1</td>
</tr>
<tr>
<td>popl09_fig3_4</td>
<td>4</td>
<td>54.7</td>
</tr>
<tr>
<td>popl09_fig4_1</td>
<td>2</td>
<td>42.7</td>
</tr>
<tr>
<td>popl09_fig4_2</td>
<td>2</td>
<td>158.3</td>
</tr>
<tr>
<td>popl09_fig4_3</td>
<td>5</td>
<td>39.2</td>
</tr>
<tr>
<td>popl09_fig4_4</td>
<td>3</td>
<td>34.2</td>
</tr>
</tbody>
</table>

**Experiment**

- 19 progs from static complexity work
- Obtain postconds representing complexity
- **Goal**: compare against results from prev work

**Results**: Obtain equiv (14) or more precise bounds (4) in 18/19 progs
Example: Verification

```c
void f(int u1, int u2) {
    assert(u1 > 0 && u2 > 0);
    int a = 1, b = 1, c = 2, d = 2;
    int x = 3, y = 3;
    int i1 = 0, i2 = 0;
    while (i1 < u1) {
        i1++;
        x = a + c; y = b + d;
        if ((x + y) % 2 == 0) {
            a++; d++;
        } else { a--;}
        i2 = 0;
        while (i2 < u2 ) {
            i2++; c--; b--; 
        }
    }
}[L] //NumInv found:
//b + 1 = c, a + 1 = d,
//a + b <= 2, 2 <= a
assert(a + c == b + d);
}
```

```c
void g(int n, int u1) {
    assert(u1 > 0);
    int x = 0;
    int m = 0;
    while (x < n) {
        m = x;
        if (u1) {
            m = x;
        }
        x = x + 1;
    }
}[L] //NumInv found:
//m^2 = nx - m - x, mn = x^2 - x
//-m <= x, x <= m + 1, n <= x
if (n > 0){
    assert(0 <= m && m < n);
}
}
```
Results: Verification

Experiment

- HOLA benchmark: 49 programs
- Various assertions (mostly postconds)
- **Goal:**
  - Obtain and compare invariants: if match or imply assertions, then assertions hold
  - Also compare with existing tool PIE
Results: Verification

Experiment

- HOLA benchmark: 49 programs
- Various assertions (mostly postconds)
- **Goal:**
  - Obtain and compare invariants: if match or imply assertions, then assertions hold
  - Also compare with existing tool PIE

**Results:** Found equiv (23) or stronger (13) invariants in 36/46 programs

- Time: mean 30s, median 13s
- Nonlinear invariants can prove many nontrivial and *unsupported* properties
NumInv

- Use CEGIR for *numerical* invariant generation
  - Dynamic Inference: use DIG to compute nonlinear invariants
  - Static Checking: use KLEE to check candidate invariants and obtain cex’s
- *Unsound*, but experience shows practical and effective in removing invalid results and can handle complex invariants
Conclusion

NumInv

- Use CEGIR for *numerical* invariant generation
  - Dynamic Inference: use DIG to compute nonlinear invariants
  - Static Checking: use KLEE to check candidate invariants and obtain cex’s
- *Unsound*, but experience shows practical and effective in removing invalid results and can handle complex invariants

Results

- Discover necessary nonlinear invariants to understand programs
- Find useful invariants capturing nontrivial runtime complexity
- Compete well with existing work
- General polynomial invariants (e.g., nonlinear properties) can *surprisingly* represent/prove many nontrivial, complex, and *unsupported* properties

https://bitbucket.org/nguyenthanhvuh/dig2/