Program Synthesis "is" Program Reachability
One-Slide Summary

- The **template-based program synthesis problem** asks if values can be found for template parameters such that the instantiated program passes all tests.

- The **program reachability problem** asks if values can be found for a set of program variables such that program execution reaches a given label.

- There is a constructive, polytime **reduction** between synthesis and reachability.
Program Repair via Synthesis

- Suppose we have a **buggy** program
  - It passes some tests and fails others
- Suppose we have **localized** the bug
  - We know which line is buggy
- Suppose we have a repair **template**
  - Fix is of the form “$x = \Box + \Box(y, \Box);$”
- Can we fill in the template so that the program passes all of the tests?
Templated Program Syntax

\[
\text{cmd} ::= \text{skip} \\
\mid \text{cmd}_1 ; \text{cmd}_2 \\
\mid v ::= \text{aexp} \\
\mid ... \\
\text{aexp} ::= \text{aexp}_1 + \text{aexp}_2 \\
\mid \text{aexp}_1 - \text{aexp}_2 \\
\mid \mathbf{c}_i \quad \text{Called a template parameter} \\
\mid ... 
\]
Template Instantiation

- Given a templated program with template parameters $c_1 \ldots c_n$, and given template values $\bar{v} = v_1 \ldots v_n$ (expressions or constants), we can instantiate, yielding a non-templated program.

- $\text{inst}(\text{skip}, \bar{v}) \rightarrow \text{skip}$

- $\text{inst}(\text{cmd}_1 ; \text{cmd}_2, \bar{v}) \rightarrow \text{inst}(\text{cmd}_1, \bar{v}) ; \text{inst}(\text{cmd}_2, \bar{v})$

- $\text{inst}(x = aexp, \bar{v}) \rightarrow x = \text{inst}(aexp, \bar{v})$

- $\text{inst}(c_i, \bar{v}) \rightarrow v_i$
Template-Based Program Synthesis

- **Given** a templated program \( P \) with template parameters \( c_1 \ldots c_n \), and a set \( T \) of input-output pairs (tests), do there exist template values \( v = v_1 \ldots v_n \) such that for all \( <\text{input, output}> \) pairs in \( T \),
  \[
  \text{inst}(P, v)(\text{input}) = \text{output} \]
Analysis

- How hard is it to solve program synthesis in general?
  - “Can you find values for these template variables such that this program passes all of its tests?”
Tools Exist: sketch

1.1 Hello World

To illustrate the process of sketching, we begin with the simplest sketch one can possibly write: the "hello world" of sketching.

```c
harness void doubleSketch(int x){
    int t = x * ??;
    assert t == x + x;
}
```

The syntax of the code fragment above should be familiar to anyone who has programmed in C or Java. The only new feature is the symbol `??`, which is Sketch syntax to represent an unknown constant. The synthesizer will replace this symbol with a suitable constant to satisfy the programmer’s requirements. In the case of this example, the programmer’s requirements are stated in the form of an assertion. The keyword harness indicates to the synthesizer that it should find a value for `??` that satisfies the assertion for all possible inputs `x`.

**Flag --bnd-inbits**  In practice, the solver only searches a bounded space of inputs ranging from zero to $2^{\text{bnd-inbits}} - 1$. The default for this flag is 5; attempting numbers much bigger than this is not recommended.

1.2 Running the synthesizer

To try this sketch out on your own, place it in a file, say `test1.sk`. Then, run the synthesizer with the following command line:

```
> sketch test1.sk
```

When you run the synthesizer in this way, the synthesized program is simply written to the console. If

1.1 Hello World

To illustrate the process of sketching, we begin with the simplest sketch one can possibly write: the "hello world" of sketching.

```
void doubleSketch(int x){
    int t = x ??;
    assert t == x + x;
}
```

The syntax of the code fragment above should be familiar to anyone who has programmed in C or Java. The only new feature is the symbol `??`, which is Sketch syntax to represent an unknown constant. The synthesizer will replace this symbol with a suitable constant to satisfy the programmer’s requirements. In the case of this example, the programmer’s requirements are stated in the form of an assertion. The keyword `harness` indicates to the synthesizer that it should find a value for `??` that satisfies the assertion for all possible inputs `x`.

**Flag `--bnd-inbits`** In practice, the solver only searches a bounded space of inputs ranging from zero to \(2^{\text{bnd-inbits}} - 1\). The default for this flag is 5; attempting numbers much bigger than this is not recommended.

1.2 Running the synthesizer

To try this sketch out on your own, place it in a file, say `test1.sk`. Then, run the synthesizer with the following command line:

```
> sketch test1.sk
```

When you run the synthesizer in this way, the synthesized program is simply written to the console. If

---

Program Synthesis as Repair

- A program synthesis algorithm can be used to solve program repair
- Conceptually: replace the buggy line with □
- If you can synthesize XYZ to fill in that hole, the patch is “delete that line and replace it with XYZ”
- In practice, template: □ = □ + □*a + □*b + □*c;
  - where a, b, c are all in-scope variables
Program Repair Example

```c
1 int is_upward(int in, int up, int down){
2     int bias, r;
3     if (in)
4         bias = down; /* fix: bias = up + 100 */
5     else
6         bias = up;
7     if (bias > down)
8         r = 1;
9     else
10        r = 0;
11     return r;
12 }
```

<table>
<thead>
<tr>
<th>Test</th>
<th>Inputs</th>
<th>Outputs</th>
<th>Passed?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>in</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>100</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>11</td>
<td>110</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>100</td>
<td>50</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>-20</td>
<td>60</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>10</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>-10</td>
</tr>
</tbody>
</table>
Program Repair Example

```c
int is_upward(int in, int up, int down) {
    int bias, r;
    if (in)
        bias = \boxed{c_0} + \boxed{c_1}*bias + \boxed{c_2}*in + \boxed{c_3}*up + \boxed{c_4}*down;
    else
        bias = up;
    if (bias > down)
        r = 1;
    else
        r = 0;
    return r;
}
```

<table>
<thead>
<tr>
<th>Test</th>
<th>in</th>
<th>up</th>
<th>down</th>
<th>expected</th>
<th>observed</th>
<th>Passed?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>0</td>
<td>✔️</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>11</td>
<td>110</td>
<td>1</td>
<td>0</td>
<td>✗</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>100</td>
<td>50</td>
<td>1</td>
<td>1</td>
<td>✔️</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>-20</td>
<td>60</td>
<td>1</td>
<td>0</td>
<td>✗</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>✔️</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>-10</td>
<td>1</td>
<td>1</td>
<td>✔️</td>
</tr>
</tbody>
</table>
Program Repair Example

```c
int is_upward(int in, int up, int down) {
    int bias, r;
    if (in)
        bias = c0 + c1 \times bias + c2 \times in + c3 \times up + c4 \times down;
    else
        bias = up;
    if (bias > down)
        r = 1;
    else
        r = 0;
    return r;
}
```

<table>
<thead>
<tr>
<th>Test</th>
<th>in</th>
<th>up</th>
<th>down</th>
<th>expected</th>
<th>observed</th>
<th>Passed?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>0</td>
<td>✓</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>11</td>
<td>110</td>
<td>1</td>
<td>0</td>
<td>✗</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>100</td>
<td>50</td>
<td>1</td>
<td>1</td>
<td>✓</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>-20</td>
<td>60</td>
<td>1</td>
<td>0</td>
<td>✗</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>✓</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>-10</td>
<td>1</td>
<td>1</td>
<td>✓</td>
</tr>
</tbody>
</table>
Program Reachability

- **Given** a program P and a set of program variables $x_1 \ldots x_n$ and a program label L, do there exist values $c_1 \ldots c_n$ such that P with $x_i$ set to $c_i$ reaches label L in finite time?

- This is what SLAM and BLAST do (repeatedly).
  - L is the error label, $c_i$ is the counterexample.

- This is what HW #5 does (repeatedly).
  - L is the end of a path, $c_i$ is the test input.
Reachability Example

```c
int x, y; /* global input */

int P() {
    if (2 * x == y)
        if (x > y + 10)
            [L]

    return 0;
}
```
Reachability Example

```c
int x, y; /* global input */

int P() {
    if (2 * x == y)
        if (x > y + 10)
            [L]

        return 0;
}
```

```plaintext
x = -20
y = -40
```
Reachability Analysis

• How hard is it to solve reachability in general?
  • “Can you find values for these variables such that this program reaches this label?”

• Many tools exist, including some that are quite mature:
  • DART, KLEE, SLAM, BLAST, PEX, CREST, CUTE, AUSTIN, “tigen”
Comparative Analysis

- Program synthesis and program reachability are both undecidable in general
- The “heart” of reachability is solving all path constraints
  - Each “if” makes it harder to find a single consistent set of values
- The “heart” of synthesis is handling all tests
  - Each new test makes it harder to find a single consistent set of values
Reductions

- Problem A is **reducible** to Problem B if an efficient algorithm for B could be used as a subroutine to solve A efficiently.
- A **gadget** is a subset of a problem instance that simulates the behavior of one of the fundamental units of a different problem.
  - Gadgets are hard to come up with the first time (e.g., when you are doing your Algo homework)
  - Gadgets often look simple once presented
Reduction Recipe

- Given an instance $I$ of problem $X$
- Assume an oracle that can solve $Y$
- Transform $I$ into $f(I)$, verify $f$ is polytime
- Let $J = Y(f(I))$
- Transform $J$ into $g(J)$, verify $g$ is polytime
- Verify $g(J) = X(I)$
- Return $g(J)$
Gadget Example

- Use Graph 3-Colorability to solve 3-SAT
- Instance shown:
  \[(x || y || !z) \&\& (!x || !y || z)\]
Gadget Example

- Use Graph 3-Colorability to solve 3-SAT
- Instance shown:
  \[(x || y || !z) \& \& (!x || !y || z)\]
Gadget Example

- Use Graph 3-Colorability to solve 3-SAT
- Instance shown:
  \[(x \lor y \lor \neg z) \land (\neg x \lor \neg y \lor z)\]
Gadget Example

- Use Graph 3-Colorability to solve 3-SAT
- Instance shown:
  \((x || y || !z) \&\& (\neg x || \neg y || z)\)
Gadget Example

- Use Graph 3-Colorability to solve 3-SAT
- Instance shown:
  \[(x \lor y \lor !z) \land (\neg x \lor \neg y \lor z)\]
Gadget Example

- Use Graph 3-Colorability to solve 3-SAT
- Instance shown:
  \[(x \lor y \lor \neg z) \land (\neg x \lor \neg y \lor z)\]
Gadget Example

- Use Graph 3-Colorability to solve 3-SAT
- Instance shown:
  \[(x || y || !z) \&\& (!x || !y || z)\]
Gadget Example

• Use Graph 3-Colorability to solve 3-SAT

• Instance shown:
  
  \((x \lor y \lor \neg z) \land (\neg x \lor \neg y \lor z)\)
Gadget Example

- Use Graph 3-Colorability to solve 3-SAT
- Instance shown:
  
  $$(x \lor y \lor \neg z) \land (\neg x \lor \neg y \lor z)$$
Gadget Example

- Use Graph 3-Colorability to solve 3-SAT
- Instance shown:
  \[(x \lor y \lor !z) \land (\neg x \lor \neg y \lor z)\]
Gadget Example

- Use Graph 3-Colorability to solve 3-SAT
- Instance shown:

\[(x \lor y \lor \neg z) \land (\neg x \lor \neg y \lor z)\]
Gadget Example

- Use Graph 3-Colorability to solve 3-SAT
- Instance shown:
  \((x \lor y \lor \neg z) \land (\neg x \lor \neg y \lor z)\)
Gadget Example

- Use Graph 3-Colorability to solve 3-SAT
- Instance shown:
  \((x \lor y \lor \neg z) \land \neg x \lor \neg y \lor z\)
- \(X = \text{true}\)
- \(Y = \text{false}\)
- \(Z = \text{true}\)
Trivia

• The *this*-Howard Isomorphism establishes a direct relationship between computer program and proofs. It shows a correspondence between proof calculi and type systems for models of computation.

<table>
<thead>
<tr>
<th>Logic side</th>
<th>Programming side</th>
</tr>
</thead>
<tbody>
<tr>
<td>axiom</td>
<td>variable</td>
</tr>
<tr>
<td>introduction rule</td>
<td>constructor</td>
</tr>
<tr>
<td>elimination rule</td>
<td>destructor</td>
</tr>
<tr>
<td>normal deduction</td>
<td>normal form</td>
</tr>
<tr>
<td>normalisation of deductions</td>
<td>weak normalisation</td>
</tr>
<tr>
<td>provability</td>
<td>type inhabitation problem</td>
</tr>
<tr>
<td>intuitionistic tautology</td>
<td>inhabited type</td>
</tr>
</tbody>
</table>
Physics

• This 1909 experiment involved tiny charged droplets of a fluid falling between two horizontal electrodes. With the electrodes uncharged, the drops reach terminal velocity while falling. By varying the voltage in the electrode plates and inducing an electromagnetic field, the drops could be perfectly suspended (electric force = gravitational force). Using the mass of the drops and the voltage, they solved for the electric charge, finding it to be always a small integer multiple of a basic constant \(1.6 \times 10^{-19} \text{ C}\): the charge of a single electron. Name the experimenter or the fluid.
Reducing Synthesis To Reachability

• Given an instance of a synthesis (repair) problem, and assuming we have an oracle that can solve reachability, let us convert the synthesis instance into a reachability instance.

• If we can do this efficiently, any existing reachability tool (e.g., DART, KLEE, SLAM) could be used to repair programs.
```c
int is_upward(int in, int up, int down) {
    int bias, r;
    if (in) {
        bias = \boxed{c_0} + \boxed{c_1} \ast \text{bias} + \boxed{c_2} \ast \text{in} + \boxed{c_3} \ast \text{up} + \boxed{c_4} \ast \text{down};
    } else {
        bias = up;
    }
    if (bias > down) {
        r = 1;
    } else {
        r = 0;
    }
    return r;
}
```

<table>
<thead>
<tr>
<th>Test</th>
<th>Inputs</th>
<th>Output</th>
<th>Passed?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>in</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>100</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>11</td>
<td>110</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>100</td>
<td>50</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>-20</td>
<td>60</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>10</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>-10</td>
</tr>
</tbody>
</table>
```c
int is_upward(int in, int up, int down) {
  int bias, r;
  if (in)
    bias = \[c_0 + c_1 * bias + c_2 * in + c_3 * up + c_4 * down\];
  else
    bias = up;
  if (bias > down)
    r = 1;
  else
    r = 0;
  return r;
}
```

<table>
<thead>
<tr>
<th>Test</th>
<th>Inputs</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>in</td>
<td>up</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>100</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>-20</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

```c
int x, y; /* global input */

int P() {
  if (2 * x == y)
    if (x > y + 10)
      [L]
      return 0;
  }
```
```
1 int is_upward(int in, int up, int down) {
2     int bias, r;
3     if (in)
4         bias = \[c_0 + c_1 \times bias + c_2 \times in + c_3 \times up + c_4 \times down; \]
5     else
6         bias = up;
7     if (bias > down)
8         r = 1;
9     else
10    r = 0;
11 return r;
12 }
```

"Heart" insights:

Multiple tests make Synthesis difficult.

Multiple path conditions make Reachability difficult.
```c
int is_upward(int in, int up, int down) {
    int bias, r;
    if (in)
        bias = c0 + c1 * bias + c2 * in + c3 * up + c4 * down;
    else
        bias = up;
    if (bias > down)
        r = 1;
    else
        r = 0;
    return r;
}

int c0, c1, c2, c3, c4; /* global input */

int pis_upward(int in, int up, int down) {
    int bias, r;
    if (in)
        bias = c0 + c1 * bias + c2 * in + c3 * up + c4 * down;
    else
        bias = up;
    if (bias > down)
        r = 1;
    else
        r = 0;
    return r;
}

int main() {
    if (pis_upward(1, 0, 100) == 0 &&
        pis_upward(1, 11, 110) == 1 &&
        pis_upward(0, 100, 50) == 1 &&
        pis_upward(1, -20, 60) == 1 &&
        pis_upward(0, 0, 10) == 0 &&
        pis_upward(0, 0, -10) == 1)
    {
        [L]
    }
    return 0;
}
```
Proving Correctness

• We must show that the constructed reachability instance is solvable (with values $c_1 \ldots c_n$) iff the original synthesis instance is solvable (with values $c_1 \ldots c_n$).

• The reachability instance is solved if those values cause execution to reach $L$.

• The synthesis instance is solved if those values cause every test to pass.
High-Level Proof Structure

- Lemma 1. The reachability instance method and the synthesis instance method agree on all (non-template) variables.

- Lemma 2. If the reachability instance reaches L from a state S (with values c1 ... cn), then that state and values model the weakest precondition of the synthesis instance method passing each test.

- Theorem 1. The synthesis instance is solvable iff the reachability instance is solvable (with the same values).
```c
1 int is_upward(int in, int up, int down) {
2     int bias, r;
3     if (in)
4         bias = \textcolor{red}{c_0} + \textcolor{red}{c_1} \times \textcolor{red}{bias} + \textcolor{red}{c_2} \times \textcolor{red}{in} + \textcolor{red}{c_3} \times \textcolor{red}{up} + \textcolor{red}{c_4} \times \textcolor{red}{down};
5     else
6         bias = \textcolor{red}{up};
7     if (bias > down)
8         r = 1;
9     else
10        r = 0;
11     return r;
12 }
```

```
```

```
```

```
```
Lemma 1 (Agree on Vars)

- Let $Q$ be the input synthesis instance method with template variables $v_1 \ldots v_n$.
- Let $P = \text{Gadget}(Q)$ be the reachability instance corresponding to method $P$.
- For all states $\sigma_1, \sigma_2, \sigma_3$, all values $c_1 \ldots c_n$, all inputs values $x$, it holds that
- If $\sigma_1(v_i) = c_i$, then $<P(x), \sigma_1> \downarrow \sigma_2$ iff $<\text{inst}(Q, \overline{c}), \sigma_1> \downarrow \sigma_3$ and for all $y \neq v_i$, $\sigma_2(y) = \sigma_3(y)$. 
Lemma 1 Proof

- If $\sigma_1(v_i) = c_i$, then $\langle P(x), \sigma_1 \rangle \downarrow \sigma_2$ iff
  $\langle \text{inst}(Q, c), \sigma_1 \rangle \downarrow \sigma_3$
  and for all $y \neq v_i$, $\sigma_2(y) = \sigma_3(y)$.

- How shall we prove it? What proof technique should we use?
Lemma 1 Proof

• If $\sigma_1(v_i) = c_i$, then $D_1 :: \langle P(x), \sigma_1 \rangle \downarrow \sigma_2$ iff $D_2 :: \langle \text{inst}(Q, \overline{c}), \sigma_1 \rangle \downarrow \sigma_3$ and for all $y \neq v_i$, $\sigma_2(y) = \sigma_3(y)$.

• The proof proceeds by induction on the structure of the operational semantics derivation $D_1$. By inversion, the structure of $D_1$ corresponds exactly to the structure of $D_2$ except for template variables.
Lemma 1 Case: Template Variable

- **Case.** Suppose $D_1$ (reachability instance) is:

  $$
  \sigma_2 = \sigma_1 [ a \rightarrow \sigma_1(v_i) ]
  $$

  $$
  < a := v_i, \sigma_1 > \downarrow \sigma_2
  $$

- By **inversion** and the construction of $P$, $D_2$ is:

  $$
  \sigma_3 = \sigma_1 [ a \rightarrow c_i ]
  $$

  $$
  < a := \text{exp}, \sigma_1 > \downarrow \sigma_3
  $$

- where $\text{exp} = \text{inst}(\boxed{c_i}, \bar{c}) = c_i$
Lemma 1 Case: Template Variable

- Have: \( \sigma_2 = \sigma_1 [ a \rightarrow \sigma_1(v_i) ] \)
- Have: \( \sigma_3 = \sigma_1 [ a \rightarrow c_i ] \)
- To show: “for all \( y \neq v_i \), \( \sigma_2(y) = \sigma_3(y) \)”
- Sub-Case 1. \( y \neq a \). Then \( \sigma_2(y) = \sigma_3(y) \).
- Sub-Case 2. \( y = a \). To show: \( \sigma_1(v_i) = c_i \). This was actually one of the assumptions in the statement of the lemma. (Intuitively, it means the reachability analysis assigned \( c_i \) to each variable \( v_i \) to reach the label L.)
Lemma 1 (Agree on Vars)

- Let $Q$ be the input synthesis instance method with template variables $v_1 \ldots v_n$.
- Let $P = \text{Gadget}(Q)$ be the reachability instance corresponding to method $P$.
- For all states $\sigma_1, \sigma_2, \sigma_3$, all values $c_1 \ldots c_n$, all inputs values $x$, it holds that
  - If $\sigma_1(v_i) = c_i$, then \( \langle P(x), \sigma_1 \rangle \downarrow \sigma_2 \iff \langle \text{inst}(Q, \overline{c}), \sigma_1 \rangle \downarrow \sigma_3 \)
  - and for all $y \neq v_i$, $\sigma_2(y) = \sigma_3(y)$.
Lemma 2 (Reach $L = \text{Pass Tests}$)

- Let $Q$ be the input synthesis instance method with template variables $v_1 \ldots v_n$ and tests $<\text{input}_1, \text{output}_1>.$
- Let $P = \text{Gadget}(Q)$ be the reachability instance method $\text{main}.$
- The execution of $P$ reaches $L$ starting from state $\sigma_1$ iff 
  $\sigma_1 \models wp(\text{result} = \text{inst}(Q, c)(\text{input}_1), \text{result} = \text{output}_1) \&\& \ldots \&\& wp(\text{result} = \text{inst}(Q, c)(\text{input}_n), \text{result} = \text{output}_n)$ where $\sigma_1(v_i) = c_i.$
Lemma 2 Proof

• By gadget construction there is only one label $L$ in $P$, “if $e$ then $[L]$” where $e$ is of the form $f(input_1) = output_1 \&\& ... f(input_n) = output_n$.

• By standard weakest precondition definitions for if, conjunction, equality and function calls, we have that $L$ is reachable iff $\sigma_1 \models wp(result = f(input_1), result = output_1) \&\& ... wp(result = f(input_n), result = output_n)$. 
Lemma 2 Proof

- Have: L is reachable iff $\sigma_1 \models wp(result = f(input_1), result = output_1) \land \ldots \land wp(result = f(input_n), result = output_n)$.

- Want: L is reachable iff $\sigma_1 \models wp(result = inst(Q, \bar{c})(input_1), result = output_1) \land \ldots \land wp(result = inst(Q, \bar{c})(input_n), result = output_n)$

- To show: $\sigma_1 \models wp(result = f(input_i), result = output_i)$ iff $\sigma_1 \models wp(result = inst(Q, \bar{c})(input_i), result = output_i)$
Lemma 2 Proof

- To show: $\sigma_1 \models wp(result = f(input_i), result = output_i)$
  iff $\sigma_1 \models wp(result = inst(Q, c)(input_i), result = output_i)$
  
  ... where $f$ is the method from Gadget($Q$)

- By the **soundness and completeness** of weakest preconditions with respect to operational semantics, we have $< result = f(input_i), \sigma_1 > \downarrow \sigma_2$ iff $\sigma_2 \models result = output_i$. 
Lemma 2 Proof

- **Have:** \(< \text{result} = f(\text{input}_i), \sigma_1 > \downarrow \sigma_2 \text{ iff } \sigma_2 |\models \text{result} = \text{output}_i.\)

- By **Lemma 1**, we have \(< \text{result} = \text{inst}(Q, \overline{c})(\text{input}_i), \sigma_1 > \downarrow \sigma_3 \text{ iff } \sigma_1(y) = \sigma_3(y) \text{ for all } y \neq v_i.\)

- Since “result” \(\neq v_i\), \(\sigma_1(\text{result}) = \sigma_3(\text{result})\) ("**Lemma1**") and \(\sigma_3(\text{result}) = \text{output}_i\) ("**Have**"). Transitively ...

- So running the template program Q instantiated with \(c_i = v_i\) on a test input produces the required output.
Correctness Theorem

• Let Q be the input synthesis instance method with template variables $v_1 \ldots v_n$ and tests $<$input$_1$, output$_n$>.  

• Let $P = \text{Gadget}(Q)$ be the reachability instance method $\text{main}$.  

• There exist parameter values $c_i$ such that for all $<$input$_i$, output$_i$>, $\text{inst}(Q,c_i)(\text{input}) = \text{output}$ iff there exist input values $t_i$ such that the execution of $P$ with $v_i \rightarrow t_i$ reaches L.  

• Proof: From Lemma 2 with $t_i = c_i$.  

Reducing Reachability To Synthesis

• We can also carry out a constructive reduction going the other direction.

• Suppose we are given an instance of program reachability. Can we convert it into a program synthesis instance to solve it?
Reachability to Synthesis Example

```c
int x, y; /* global input */

int P() {
    if (2 * x == y)
        if (x > y + 10)
            [L]
    return 0;
}
```

```c
int is_upward(int in, int up, int down){
    int bias, r;
    if (in)
        bias = $c_0 + c_1*bias + c_2*in + c_3*up + c_4*down$;
    else
        bias = up;
    if (bias > down)
        r = 1;
    else
        r = 0;
    return r;
}
```

<table>
<thead>
<tr>
<th>Test</th>
<th>Inputs</th>
<th>Output</th>
<th>Passed?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>in</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>100</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>11</td>
<td>110</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>100</td>
<td>50</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>-20</td>
<td>60</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>10</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>-10</td>
</tr>
</tbody>
</table>
Reachability to Synthesis Example

```c
int x, y; /* global input */

int P() {
    if (2 * x == y)
        if (x > y + 10)
            [L]
    return 0;
}

int qP() {
    if (2 * x == y)
        if (x > y + 10)
            /* location of [L] in P */
            raise REACHED;
    return 0;
}

int qmain() {
    /* Find x and y. Equivalently, synthesize:
       x = c_x
       y = c_y */
    try {
        qP();
    } catch (REACHED) {
        return 1;
    }
    return 0;
}

Test suite: Q() = 1
```
Implications

• Program reachability tools are much more mature than program repair tools.

• CETI Program Repair Algorithm
  • For each buggy line, in ranked order
    – For every repair template, in ranked order
      • Convert repair instance to reachability instance
      • Call off-the-shelf reachability tool (e.g., SMT solver / KLEE)
      • If reachable, return parameters as patch
Prototype CETI Evaluation

- Considered 41 bugs and simple one-line templates
- Fixed 100% of bugs admitting one-line fixes
- 22 seconds each, average
- Debroy & Wong (random mutation): 9 repairs
- GenProg: 11 repairs
- Forensic (concolic execution): 23 repairs
- CETI: 26 repairs
Concluding Thoughts

- PL Theory almost always translates into useful PL Practice (just with an X year lag time)
- There is plenty of scope for insight and creativity (e.g., whence these gadgets?)
- Techniques like structural induction, SMT solving, fault localization, substitution, axiomatic semantics, etc., remain relevant!
- HW0 (BLAST), HW5 (tigen), FlashFill (Gulwani Excel) and GenProg (last lecture) are all “secretly the same thing”
  = “statically reason about dynamic execution”