Software Testing, Quality Assurance and Maintenance Winter 2017

Lecture 32 — March 24, 2017

Patrick Lam *version 0 – DRAFT, not finished yet*

Static analysis tools for Java that you can download

FindBugs. An open-source static bytecode analyzer for Java out of the University of Maryland.

`findbugs.sourceforge.net`

It's like PMD in finding bug patterns:

- off-by-one;
- null pointer dereference;
- ignored `read()` return value;
- ignored return value (immutable classes);
- uninitialized read in constructor;
- and more…

A key difference is that it performs static analysis at Java bytecode level. It's therefore harder to write FindBugs rules.

You can read a comparison of different tools in this paper:

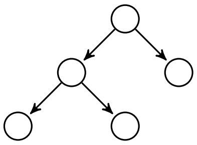
`http://www.cs.umd.edu/~jfoster/papers/issre04.pdf`

FindBugs gives some false positives. Here are some techniques to help avoid them:

`patricklam.ca/papers/14.msr.saa.pdf`

Korat (University of Illinois). Key Idea: Generate Java objects from a representation invariant specification written as a Java method.

For instance, here's a binary tree.



Binary Tree!

One characteristic of a binary tree:

- left & right pointers don't refer to same node.

We can express that characteristic in Java as follows:

```
boolean repOk() {
  if (root == null) return size == 0;                // empty tree has size 0
  Set visited = new HashSet(); visited.add(root);
  List workList = new LinkedList(); workList.add(root);
  while (!workList.isEmpty()) {
    Node current = (Node)workList.removeFirst();
    if (current.left != null) {
      if (!visited.add(current.left)) return false; // acyclicity
      workList.add(current.left);
    }
    if (current.right != null) {
      if (!visited.add(current.right)) return false; // acyclicity
      workList.add(current.right);
    }
  }
  if (visited.size() != size) return false;          // consistency of size
  return true;
}
```

Korat then generates all distinct (“non-isomorphic”) trees, up to a given size (say 3). It uses these trees as inputs for testing the `add()` method of the tree (or for any other methods.)

`korat.sourceforge.net/index.html`