**Task 2: Dead Function Analysis**

|  |  |  |
| --- | --- | --- |
| **Chew Yung Chung** a0133662J  a0133662@u.nus.edu | **Tan Qiu Hao, Joel** a0125473H  a0125473@u.nus.edu | **Juliana Seng** a0126332R  a0126332@u.nus.edu |

# Implementation and Algorithm

The algorithm maintains several global objects that are collated from 1 or more IR files, they are as follows:

* mainList - holds a list of function pointers to main() functions
* programFuncMap - maps function name to DEAD or LIVE status
* definedFuncMap - maps function name to function pointers
* pointerFuncMap - maps key variable name to function pointers

Firstly, mainList is populated by iterating through all the functions and filtering functions with the function name “main”.

At the same time, programFuncMap is populated by storing all retrieved functions with an initial status of DEAD, and definedFuncMap stores the mapping of the retrieved function names to their respective pointer.

A triple nested for-loop is then executed to iterate through all the instructions that are reachable through the main() functions stored in the mainList. The code is as follows:

|  |  |
| --- | --- |
| 64  65  66  67  68  69  70  71  72  73  74  75  76  77  78  79  80  81  82 | For (auto &F : mainList) {  for (auto &BB: \*F) {  for (auto &I : BB) {  StoreInst \*S = dyn\_cast<StoreInst>(&I);  if (S) InvestigateStoreInst(S);  CallSite Call(&I);  if (!Call) continue;  Function \*G = Call.getCalledFunction();  if (G == nullptr) {  G = ResolveIndirectCall(Call);  if (G == nullptr) continue;  }  programFuncMap[G->getName()] = "LIVE";  if (definedFuncMap[G->getName()] != 0) {  InvestigateFunction(\*(definedFuncMap[G->getName()]));  }  }  }  } |

*Code snippet from asg2-task1.cpp*

If the instruction is a store instruction, the InvestigateStoreInst() function is invoked to map the name of the variable to function pointer. InvestigateStoreInst() also recognize that it is possible for a pointer to be not mapped directly to a function, but through other layers of pointer. Hence a do-while loop is utilized to iterate through all pointers, until a function or null value is reached. The information is then stored in pointerFuncMap.

If the instruction is a call instruction, the name of the called function is retrieved. However, if a null value is retrieved, the call may be referencing a function pointer, hence ResolveIndirectCall() is invoked to iterate through the pointerFuncMap, that was built previously, to retrieve the function name.

The status of the called function is subsequently set to LIVE in programFuncMap. Alternatively, if the called function is referenced with a function pointer, InvestigateFunction() is invoked to set its status to LIVE.

Finally, programFuncMap is iterated though and all functions with a DEAD status is retrieved and reported accordingly.

# Build and Run

Run build.sh to compile the test cases, program and execute the test cases.

|  |
| --- |
| $ ./build.sh |

The individual commands can also be found in build.sh.

An expected output of the shell code is as follows, all warnings are truncated.

|  |
| --- |
| ----------COMPILING TESTCASES----------  ----------COMPILING PROGRAM----------  ----------RUNNING TEST 1----------  ----------RUNNING TEST 2----------  WARNING: function <dead2\_dead\_function> is a DEAD function  WARNING: function <dead2\_function\_always\_called> is a DEAD function  WARNING: function <dead2\_complex\_function> is a DEAD function  WARNING: function <dead2\_maybe\_dead\_function> is a DEAD function  ----------RUNNING TEST 3----------  ----------RUNNING TEST 4----------  ----------RUNNING TEST 5----------  WARNING: function <foo1> is a DEAD function  WARNING: function <foo2> is a DEAD function |

# Test Cases

Test case 1: Function pointer

|  |
| --- |
| $ ./asg2-task1 dead.ll |

Test case 1 observes the behaviour of dead.c as follows

|  |  |
| --- | --- |
| 20  21  22  23  24  25  26  27  28  29  30  31  32  33  34  35  36  37  38 | if (complex\_function()) {  maybe\_dead\_function();  }  function\_always\_called();  if (0) {  dead\_function();  }  if (dead2\_complex\_function()) {  dead2\_maybe\_dead\_function();  }  dead2\_function\_always\_called();  if (0) {  dead2\_dead\_function();  }  f = &dead\_function;  f(); |

*Code snippet from dead.c*

Dead.c defines 4 functions, namely

* complex\_function(), a function that randomly returns true or false
* maybe\_dead\_function()
* function\_always\_called()
* dead\_function()

It also demonstrates the initiation and invocation of a function pointer to dead\_function(). All functions are LIVE.

Test case 2: No main function

|  |
| --- |
| $ ./asg2-task1 dead2.ll |

Test case 2 observes the behaviour of dead2.c, which does not contain a main() function, but however, defines 4 functions as follows

* dead2\_complex\_function(), a function that randomly returns true or false
* dead2\_maybe\_dead\_function()
* dead2\_function\_always\_called()
* dead2\_dead\_function()

However, as none was called, all 4 functions were detected as dead functions.

Test case 3: Multiple IR files

|  |
| --- |
| $ ./asg2-task1 dead.ll dead2.ll |

Test case 3 observes the input of multiple files, namely dead.c and dead2.c, as described above. Functions that were defined in dead2.c that were previously not called, are invoked in dead.c, hence all functions are LIVE.

Test case 4: More function pointers

|  |
| --- |
| $ ./asg2-task1 dead3.ll |

Test case 4 demonstrates more examples on function calls through function pointers.

Test case 5: Recursive function

|  |
| --- |
| $ ./asg2-task1 dead4.ll |

Test case 5 observes the behaviour of having 2 functions that recursively call each other, but is not invoked from main(). Although the 2 functions reference each other, they are detected as dead functions as they were not called from main().

# Limitations

Much consideration was made to design the test cases, however, there are some corner cases that were made aware to us, and that the algorithm can improve on in future.

|  |
| --- |
| if (!(x == 0 || 0 == 0)) {  test1();  } |

Although 0=0 will always evaluate to true, causing the if-statement to be false and its contents be never executed, test1() is not detected as a dead function.

|  |
| --- |
| if (!(x == x)) {  test2();  } |

A warning will be raised, as x==x will always evaluate to true, causing the if-statement to be false and its contents be never executed, however, test2() is not detected as a dead function. Nevertheless, if the variable x is replaced by a value, for example, 5==5, the algorithm will then be able to detect test2() as a dead function.

|  |
| --- |
| for (int y = 0; y < 0; y++) {  test3();  } |

The for-loop will fail the condition in the first iteration, hence it will not be entered at all and its contents be never executed, however, test3() is not detected as a dead function.