**Implicit larval state verification examples**

Testing methodology :

1. Develope a test in java.
2. Generate bytecode by compiling with javac
3. Disassemble .class file to .jasm file.

java -cp . -jar asmtools.jar jdis test\_larval.class > test\_larval.jasm

1. modify jasm file
2. assemble back to .class file.

java -cp . -jar asmtools.jar jasm test\_larval.jasm > test\_larval.class

1. run JVM while will perform bytecode verification during linking.

**Case 1) Passing uninitializedThis to a method expecting a type argument.**

public static Method main:"([Ljava/lang/String;)V"

stack 4 locals 2

{

new class MyValue;

astore\_1;

getstatic Field java/lang/System.out:"Ljava/io/PrintStream;";

aload\_1;

invokestatic Method micro:"(LMyValue;)I"; //// 🡪 UninitializedThis passed to static method.

invokedynamic InvokeDynamic REF\_invokeStatic:Method java/lang/invoke/StringConcatFactory.makeConcatWithConstants:

"(Ljava/lang/invoke/MethodHandles$Lookup;Ljava/lang/String;Ljava/lang/invoke/MethodType;Ljava/lang/String;[Ljava/lang/Object;)Ljava/lang/invoke/CallSite;":

makeConcatWithConstants:"(I)Ljava/lang/String;" {

String "[res] \u0001"

};

invokevirtual Method java/io/PrintStream.println:"(Ljava/lang/String;)V";

return;

}

CPROMPT>java --enable-preview -cp . test\_larval

Error: Unable to initialize main class test\_larval

Caused by: java.lang.VerifyError: Bad type on operand stack

Exception Details:

Location:

test\_larval.main([Ljava/lang/String;)V @8: invokestatic

Reason:

Type uninitialized 0 (current frame, stack[1]) is not assignable to 'MyValue'

Current Frame:

bci: @8

flags: { }

locals: { '[Ljava/lang/String;', uninitialized 0 }

stack: { 'java/io/PrintStream', uninitialized 0 }

Bytecode:

0000000: bb00 024c b200 042b b800 05ba 0006 0000

0000010: b600 07b1

**Case 2) Passing initialized instance to a constructor expecting to receive an uninitializedThis on stack frame.**

public static Method main:"([Ljava/lang/String;)V"

stack 4 locals 2

{

new class MyValue;

dup;

bipush 10;

bipush 20;

invokespecial Method MyValue."<init>":"(II)V";

dup;

bipush 10;

bipush 20;

invokespecial Method MyValue."<init>":"(II)V";

astore\_1;

getstatic Field java/lang/System.out:"Ljava/io/PrintStream;";

aload\_1;

invokestatic Method micro:"(LMyValue;)I";

invokedynamic InvokeDynamic REF\_invokeStatic:Method java/lang/invoke/StringConcatFactory.makeConcatWithConstants:

"(Ljava/lang/invoke/MethodHandles$Lookup;Ljava/lang/String;Ljava/lang/invoke/MethodType;Ljava/lang/String;[Ljava/lang/Object;)Ljava/lang/invoke/CallSite;":

makeConcatWithConstants:"(I)Ljava/lang/String;" {

String "[res] \u0001"

};

invokevirtual Method java/io/PrintStream.println:"(Ljava/lang/String;)V";

return;

}

CPROMPT>java --enable-preview -cp . test\_larval

Error: Unable to initialize main class test\_larval

Caused by: java.lang.VerifyError: Bad operand type when invoking <init>

Exception Details:

Location:

test\_larval.main([Ljava/lang/String;)V @16: invokespecial

Reason:

Invalid type: 'MyValue' (current frame, stack[1])

Current Frame:

bci: @16

flags: { }

locals: { '[Ljava/lang/String;' }

stack: { 'MyValue', 'MyValue', integer, integer }

Bytecode:

0000000: bb00 0259 100a 1014 b700 0459 100a 1014

0000010: b700 044c b200 052b b800 06ba 0007 0000

0000020: b600 08b1

**Case 3) Accessing a field of an uninitialzedThis**

public static Method main:"([Ljava/lang/String;)V"

stack 4 locals 2

{

new class MyValue;

astore\_1;

getstatic Field java/lang/System.out:"Ljava/io/PrintStream;";

aload\_1;

getfield Field MyValue.field1:"I";

invokedynamic InvokeDynamic REF\_invokeStatic:Method java/lang/invoke/StringConcatFactory.makeConcatWithConstants:

"(Ljava/lang/invoke/MethodHandles$Lookup;Ljava/lang/String;Ljava/lang/invoke/MethodType;Ljava/lang/String;[Ljava/lang/Object;)Ljava/lang/invoke/CallSite;":

makeConcatWithConstants:"(I)Ljava/lang/String;" {

String "[field1\u0001"

};

getstatic Field java/lang/System.out:"Ljava/io/PrintStream;";

aload\_1;

bipush 10;

bipush 20;

invokespecial Method MyValue."<init>":"(II)V";

invokevirtual Method java/io/PrintStream.println:"(Ljava/lang/String;)V";

getstatic Field java/lang/System.out:"Ljava/io/PrintStream;";

aload\_1;

invokestatic Method micro:"(LMyValue;)I";

invokedynamic InvokeDynamic REF\_invokeStatic:Method java/lang/invoke/StringConcatFactory.makeConcatWithConstants:

"(Ljava/lang/invoke/MethodHandles$Lookup;Ljava/lang/String;Ljava/lang/invoke/MethodType;Ljava/lang/String;[Ljava/lang/Object;)Ljava/lang/invoke/CallSite;":

makeConcatWithConstants:"(I)Ljava/lang/String;" {

String "[res] \u0001"

};

invokevirtual Method java/io/PrintStream.println:"(Ljava/lang/String;)V";

return;

}

CPROMPT>java --enable-preview -cp . test\_larval

Error: Unable to initialize main class test\_larval

Caused by: java.lang.VerifyError: Bad type on operand stack

Exception Details:

Location:

test\_larval.main([Ljava/lang/String;)V @8: getfield

Reason:

Type uninitialized 0 (current frame, stack[1]) is not assignable to 'MyValue'

Current Frame:

bci: @8

flags: { }

locals: { '[Ljava/lang/String;', uninitialized 0 }

stack: { 'java/io/PrintStream', uninitialized 0 }

Bytecode:

0000000: bb00 024c b200 042b b400 05ba 0006 0000

0000010: b200 042b 100a 1014 b700 07b6 0008 b200

0000020: 042b b800 09ba 000a 0000 b600 08b1

**Case 4) Updating the filed of an uninitializedThis**

public static Method main:"([Ljava/lang/String;)V"

stack 4 locals 2

{

new class MyValue;

astore\_1;

aload\_1;

iconst\_1;

putfield Field MyValue.field1:"I";

aload\_1;

bipush 10;

bipush 20;

invokespecial Method MyValue."<init>":"(II)V";

getstatic Field java/lang/System.out:"Ljava/io/PrintStream;";

aload\_1;

getfield Field MyValue.field1:"I";

invokedynamic InvokeDynamic REF\_invokeStatic:Method java/lang/invoke/StringConcatFactory.makeConcatWithConstants:

"(Ljava/lang/invoke/MethodHandles$Lookup;Ljava/lang/String;Ljava/lang/invoke/MethodType;Ljava/lang/String;[Ljava/lang/Object;)Ljava/lang/invoke/CallSite;":

makeConcatWithConstants:"(I)Ljava/lang/String;" {

String "[field1\u0001"

};

invokevirtual Method java/io/PrintStream.println:"(Ljava/lang/String;)V";

getstatic Field java/lang/System.out:"Ljava/io/PrintStream;";

aload\_1;

invokestatic Method micro:"(LMyValue;)I";

invokedynamic InvokeDynamic REF\_invokeStatic:Method java/lang/invoke/StringConcatFactory.makeConcatWithConstants:

"(Ljava/lang/invoke/MethodHandles$Lookup;Ljava/lang/String;Ljava/lang/invoke/MethodType;Ljava/lang/String;[Ljava/lang/Object;)Ljava/lang/invoke/CallSite;":

makeConcatWithConstants:"(I)Ljava/lang/String;" {

String "[res] \u0001"

};

invokevirtual Method java/io/PrintStream.println:"(Ljava/lang/String;)V";

return;

}

CPROMPT>java --enable-preview -cp . test\_larval

Error: Unable to initialize main class test\_larval

Caused by: java.lang.VerifyError: Bad type on operand stack in putfield

Exception Details:

Location:

test\_larval.main([Ljava/lang/String;)V @6: putfield

Reason:

Type uninitialized 0 (current frame, stack[0]) is not assignable to 'MyValue' (constant pool 4)

Current Frame:

bci: @6

flags: { }

locals: { '[Ljava/lang/String;', uninitialized 0 }

stack: { uninitialized 0, integer }

Bytecode:

0000000: bb00 024c 2b04 b500 042b 100a 1014 b700

0000010: 05b2 0006 2bb4 0004 ba00 0700 00b6 0008

0000020: b200 062b b800 09ba 000a 0000 b600 08b1

0000030:

**Case 5) Returning an uninitialized object**

public static Method micro:"(II)LMyValue;"

stack 4 locals 3

{

new class MyValue;

astore\_2;

aload\_2;

areturn;

}

public static Method main:"([Ljava/lang/String;)V"

stack 2 locals 2

{

bipush 10;

bipush 20;

invokestatic Method micro:"(II)LMyValue;";

astore\_1;

getstatic Field java/lang/System.out:"Ljava/io/PrintStream;";

aload\_1;

getfield Field MyValue.field1:"I";

invokedynamic InvokeDynamic REF\_invokeStatic:Method java/lang/invoke/StringConcatFactory.makeConcatWithConstants:

"(Ljava/lang/invoke/MethodHandles$Lookup;Ljava/lang/String;Ljava/lang/invoke/MethodType;Ljava/lang/String;[Ljava/lang/Object;)Ljava/lang/invoke/CallSite;":

makeConcatWithConstants:"(I)Ljava/lang/String;" {

String "[field1\u0001"

};

invokevirtual Method java/io/PrintStream.println:"(Ljava/lang/String;)V";

return;

}

CPROMPT>java --enable-preview -cp . test\_larval

Error: Unable to initialize main class test\_larval

Caused by: java.lang.VerifyError: Bad return type

Exception Details:

Location:

test\_larval.micro(II)LMyValue; @5: areturn

Reason:

Type uninitialized 0 (current frame, stack[0]) is not assignable to 'MyValue' (from method signature)

Current Frame:

bci: @5

flags: { }

locals: { integer, integer, uninitialized 0 }

stack: { uninitialized 0 }

Bytecode:

0000000: bb00 024d 2cb0

**Case 6) Assigning an uninitialized instance to a reference of same type.**

public static Method micro:"(II)LMyValue;"

stack 4 locals 4

{

new class MyValue;

astore\_2;

aload\_2;

astore\_3;

aload\_2;

dup;

iload\_0;

iload\_1;

invokespecial Method MyValue."<init>":"(II)V";

areturn;

}

public static Method main:"([Ljava/lang/String;)V"

stack 2 locals 2

{

bipush 10;

bipush 20;

invokestatic Method micro:"(II)LMyValue;";

astore\_1;

getstatic Field java/lang/System.out:"Ljava/io/PrintStream;";

aload\_1;

getfield Field MyValue.field1:"I";

invokedynamic InvokeDynamic REF\_invokeStatic:Method java/lang/invoke/StringConcatFactory.makeConcatWithConstants:

"(Ljava/lang/invoke/MethodHandles$Lookup;Ljava/lang/String;Ljava/lang/invoke/MethodType;Ljava/lang/String;[Ljava/lang/Object;)Ljava/lang/invoke/CallSite;":

makeConcatWithConstants:"(I)Ljava/lang/String;" {

String "[field1\u0001"

};

invokevirtual Method java/io/PrintStream.println:"(Ljava/lang/String;)V";

return;

}

CPROMPT>java --enable-preview -cp . test\_larval

[field110

Inference: Assignments are translated into stack load and store operations and as long as unassigned reference is not passed to another context it does not result into a verification error.

public static Method micro:"(II)LMyValue;"

stack 4 locals 4

{

new class MyValue;

astore\_2;

aload\_2;

astore\_3;

getstatic Field java/lang/System.out:"Ljava/io/PrintStream;";

aload\_3;

invokestatic Method java/lang/String.valueOf:"(Ljava/lang/Object;)Ljava/lang/String;";

invokedynamic InvokeDynamic REF\_invokeStatic:Method java/lang/invoke/StringConcatFactory.makeConcatWithConstants:

"(Ljava/lang/invoke/MethodHandles$Lookup;Ljava/lang/String;Ljava/lang/invoke/MethodType;Ljava/lang/String;[Ljava/lang/Object;)Ljava/lang/invoke/CallSite;":

makeConcatWithConstants:"(Ljava/lang/String;)Ljava/lang/String;" {

String "obj => \u0001"

};

invokevirtual Method java/io/PrintStream.println:"(Ljava/lang/String;)V";

aload\_2;

iload\_0;

iload\_1;

invokespecial Method MyValue."<init>":"(II)V";

areturn;

}

CPROMPT>java --enable-preview -cp . test\_larval

Error: Unable to initialize main class test\_larval

Caused by: java.lang.VerifyError: Bad type on operand stack

Exception Details:

Location:

test\_larval.micro(II)LMyValue; @10: invokestatic

Reason:

Type uninitialized 0 (current frame, stack[1]) is not assignable to 'java/lang/Object'

Current Frame:

bci: @10

flags: { }

locals: { integer, integer, uninitialized 0, uninitialized 0 }

stack: { 'java/io/PrintStream', uninitialized 0 }

Bytecode:

0000000: bb00 024d 2c4e b200 032d b800 04ba 0005

0000010: 0000 b600 062c 1a1b b700 07b0

**Case 7) Casting an uninitialized instance using checkcast.**

public static Method micro:"(II)LMyValue;"

stack 4 locals 4

{

new class MyValue;

astore\_2;

aload\_2;

checkcast class MyValue;

astore\_3;

aload\_2;

iload\_0;

iload\_1;

invokespecial Method MyValue."<init>":"(II)V";

areturn;

}

CPROMPT>java --enable-preview -cp . test\_larval

Error: Unable to initialize main class test\_larval

Caused by: java.lang.VerifyError: Bad type on operand stack

Exception Details:

Location:

test\_larval.micro(II)LMyValue; @5: checkcast

Reason:

Type uninitialized 0 (current frame, stack[0]) is not assignable to 'java/lang/Object'

Current Frame:

bci: @5

flags: { }

locals: { integer, integer, uninitialized 0 }

stack: { uninitialized 0 }

Bytecode:

0000000: bb00 024d 2cc0 0002 4e2c 1a1b b700 03b0

0000010:

**Case 8) Meeting of uninitialzedThis and initialized instance at a convergence point.**

public static Method micro:"(II)LMyValue;"

stack 4 locals 3

{

aconst\_null;

astore\_2;

iload\_0;

iload\_1;

if\_icmple L20;

new class MyValue;

astore\_2;

goto L30;

L20: stack\_frame\_type append;

locals\_map class MyValue;

new class MyValue;

dup;

iload\_1;

iload\_0;

invokespecial Method MyValue."<init>":"(II)V";

astore\_2;

L30: stack\_frame\_type same;

aload\_2;

areturn;

}

CPROMPT>java --enable-preview -cp . test\_larval

Error: Unable to initialize main class test\_larval

Caused by: java.lang.VerifyError: Inconsistent stackmap frames at branch target 24

Exception Details:

Location:

test\_larval.micro(II)LMyValue; @24: aload\_2

Reason:

Type uninitialized 7 (current frame, locals[2]) is not assignable to 'MyValue' (stack map, locals[2])

Current Frame:

bci: @11

flags: { }

locals: { integer, integer, uninitialized 7 }

stack: { }

Stackmap Frame:

bci: @24

flags: { }

locals: { integer, integer, 'MyValue' }

stack: { }

Bytecode:

0000000: 014d 1a1b a400 0abb 0002 4da7 000d bb00

0000010: 0259 1b1a b700 034d 2cb0

Stackmap Table:

append\_frame(@14,Object[#2])

same\_frame(@24)

**Larval values generated using Unsafe makePrivateBuffer should adhere to the same semantics as uninitialized instance generated by new bytecode.**