QR code repository

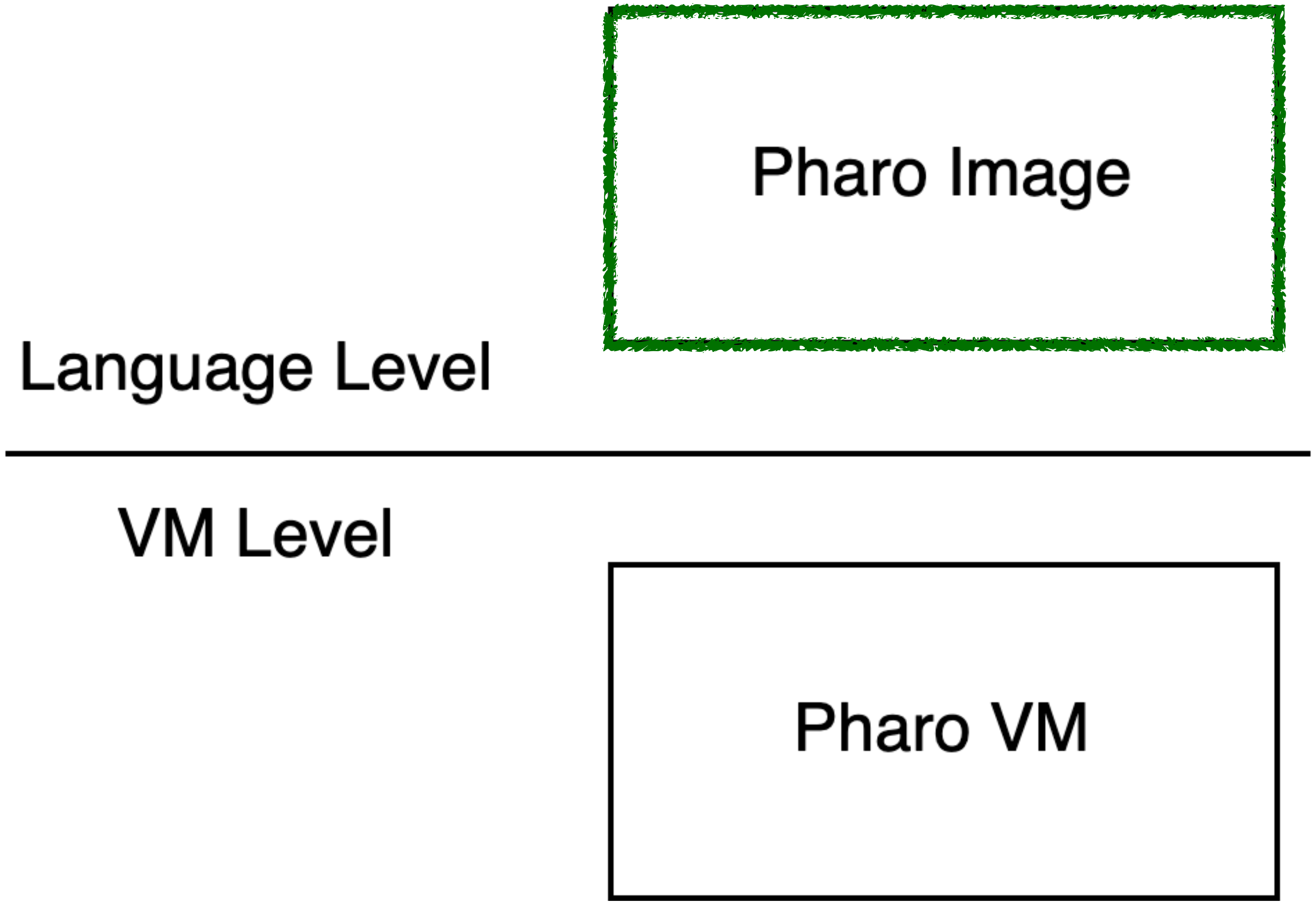
Polyphemus

Ease Virtual Machine Level Tooling

Pierre Misse-Chanabier & Theo Rogliano

Who does not love tools ?

Tools at the language level



Pharo Image

Language Level

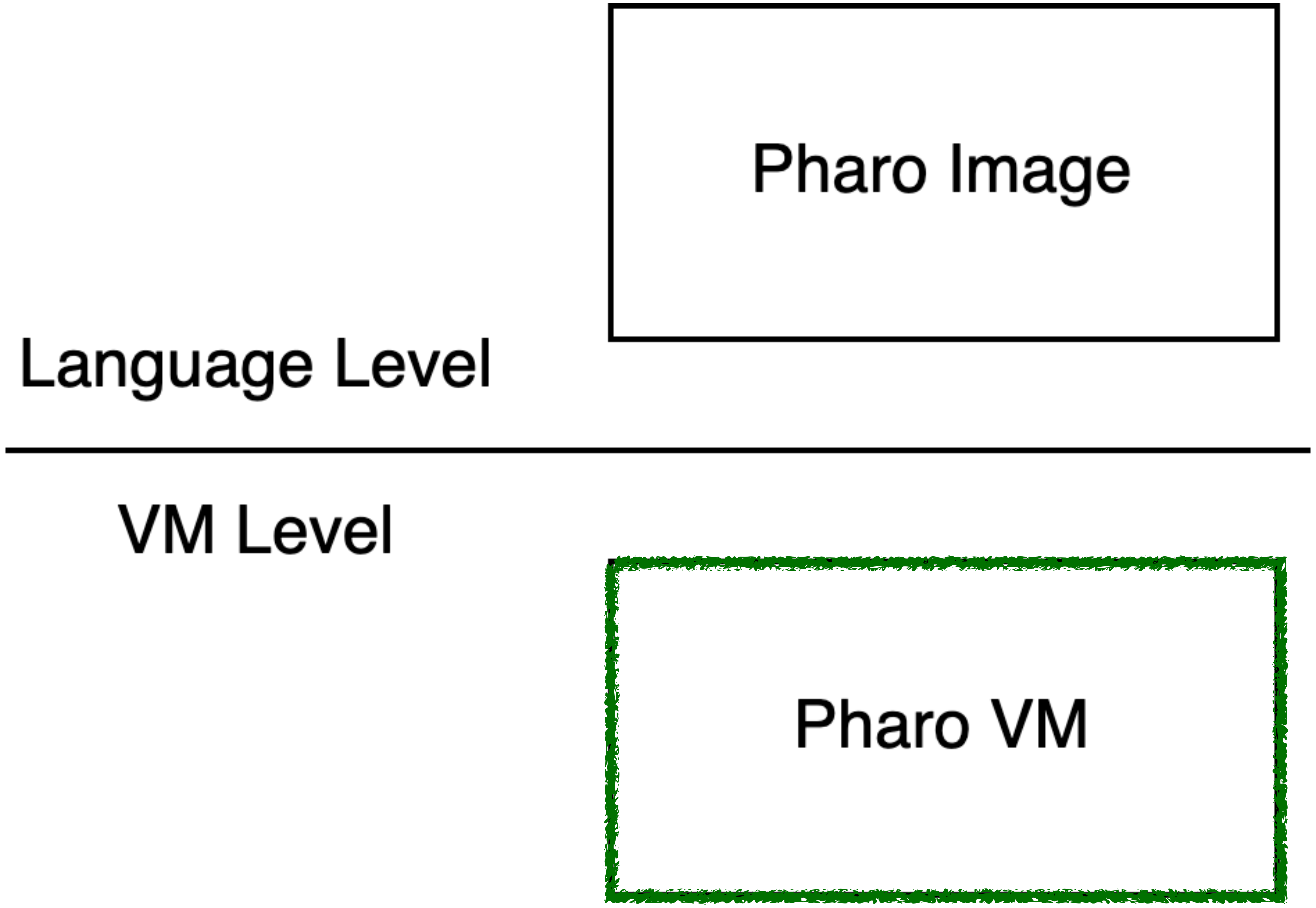
VM Level

Pharo VM

NewTools, Moose, Roassal,
Calypso, SUnit, Iceberg, Refactoring, Epicea
… … …

Who does not love tools ?

Tools at the VM level



Pharo Image

Language Level

VM Level

Pharo VM

Bootstrap, VM machine code debugger

…

Who does not love tools ?

Why should we care about VM level tools ?

```
Form >> #scaledByDisplayScaleFactor
            1 halt.
            ^ self scaledToSize: self extent * self currentWorld displayScaleFactor.
```

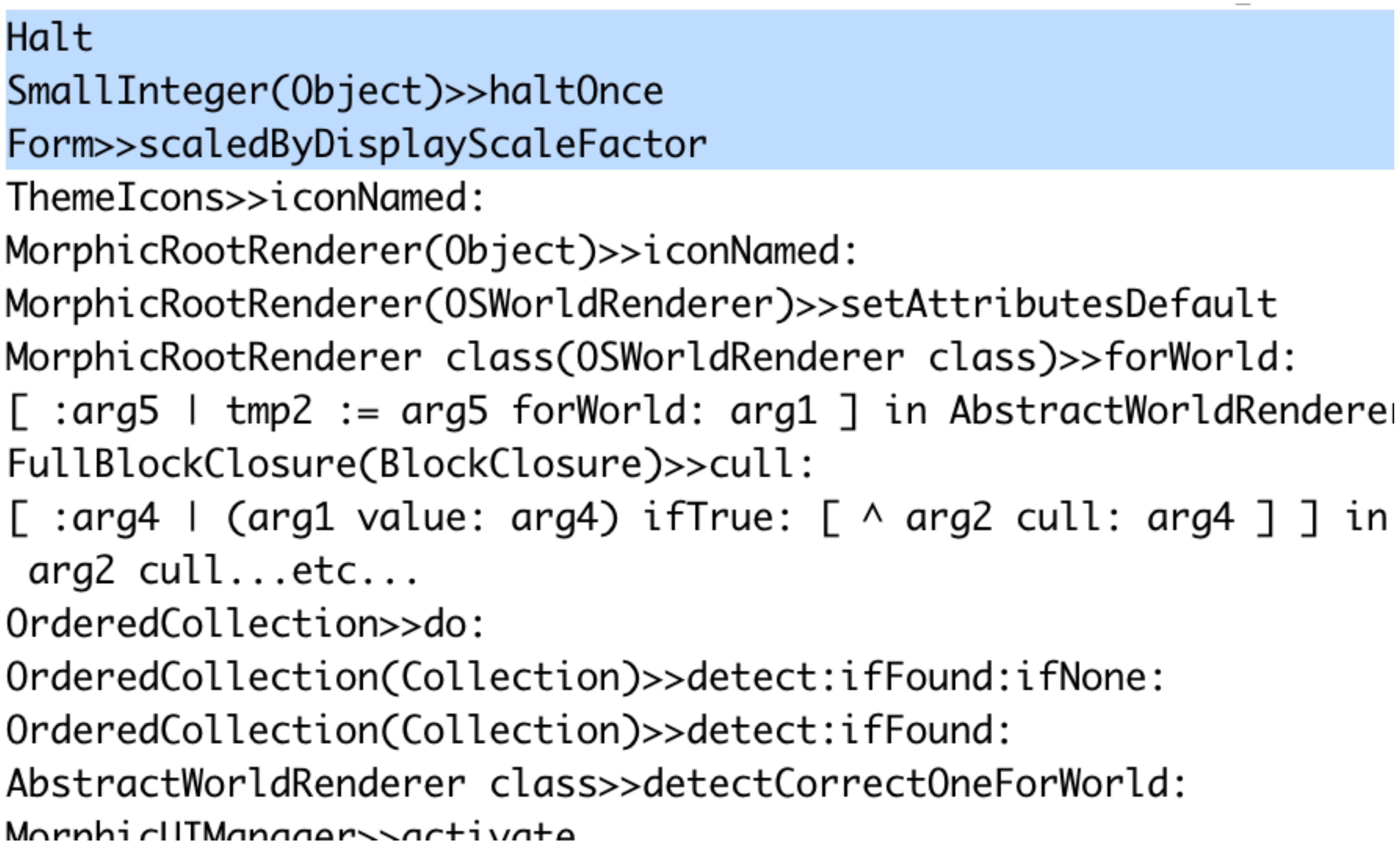
Who does not love tools ?

Don’t save it !

```
Form >> #scaledByDisplayScaleFactor
        1 halt.
        ^ self scaledToSize: self extent * self currentWorld displayScaleFactor.
```

Who does not love tools ?

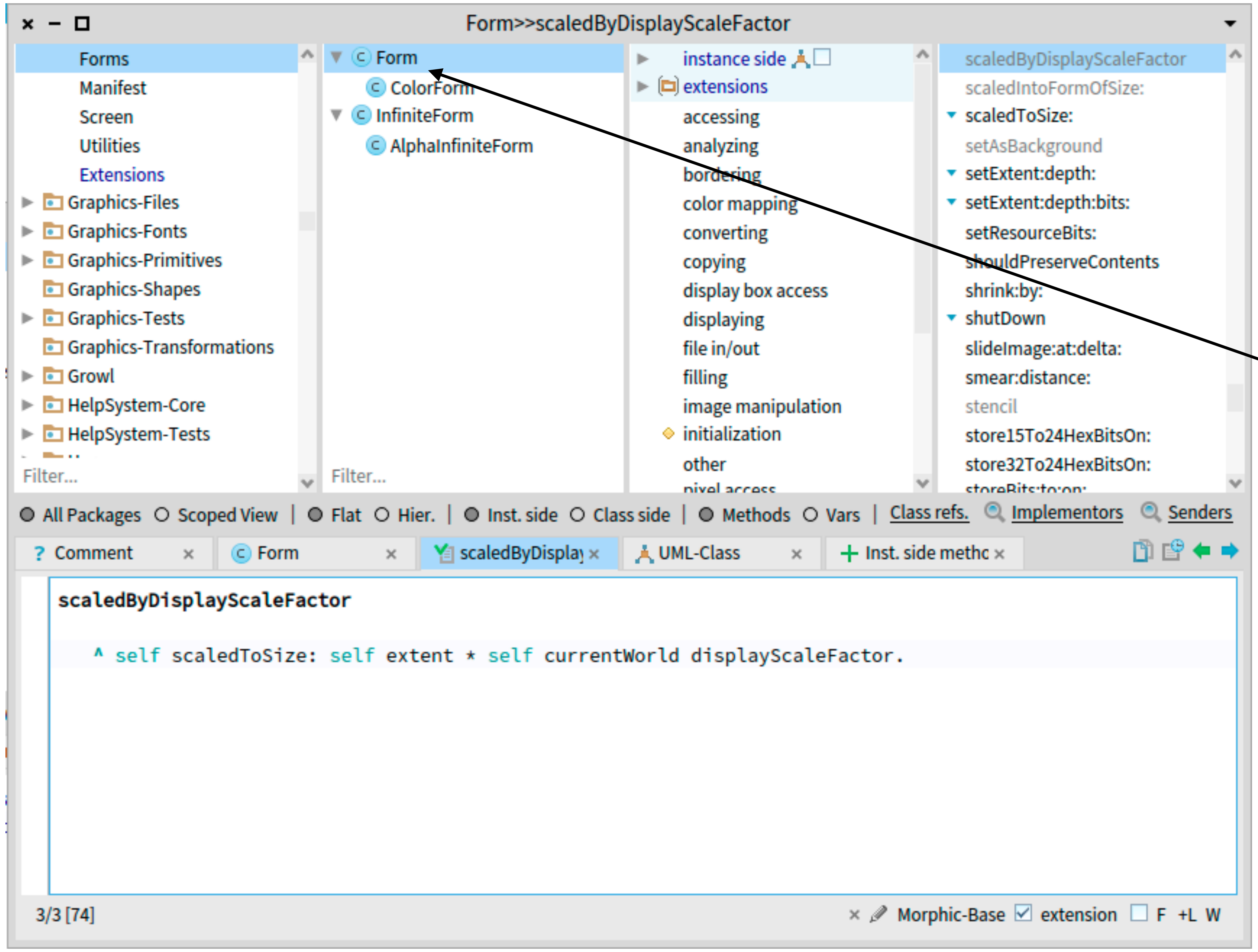
Too late !



```
Halt
SmallInteger(Object)>>haltOnce
Form>>scaledByDisplayScaleFactor
ThemeIcons>>iconNamed:
MorphicRootRenderer(Object)>>iconNamed:
MorphicRootRenderer(OSWorldRenderer)>>setAttributesDefault
MorphicRootRenderer class(OSWorldRenderer class)>>forWorld:
[ :arg5 | tmp2 := arg5 forWorld: arg1 ] in AbstractWorldRendere
FullBlockClosure(BlockClosure)>>cull:
[ :arg4 | (arg1 value: arg4) ifTrue: [ ^ arg2 cull: arg4 ] ] in
 arg2 cull...etc...
OrderedCollection>>do:
OrderedCollection(Collection)>>detect:ifFound:ifNone:
OrderedCollection(Collection)>>detect:ifFound:
AbstractWorldRenderer class>>detectCorrectOneForWorld:
MorphicUIManager>>activate
```

Let’s do VM level tools !

Let’s find the class Form …



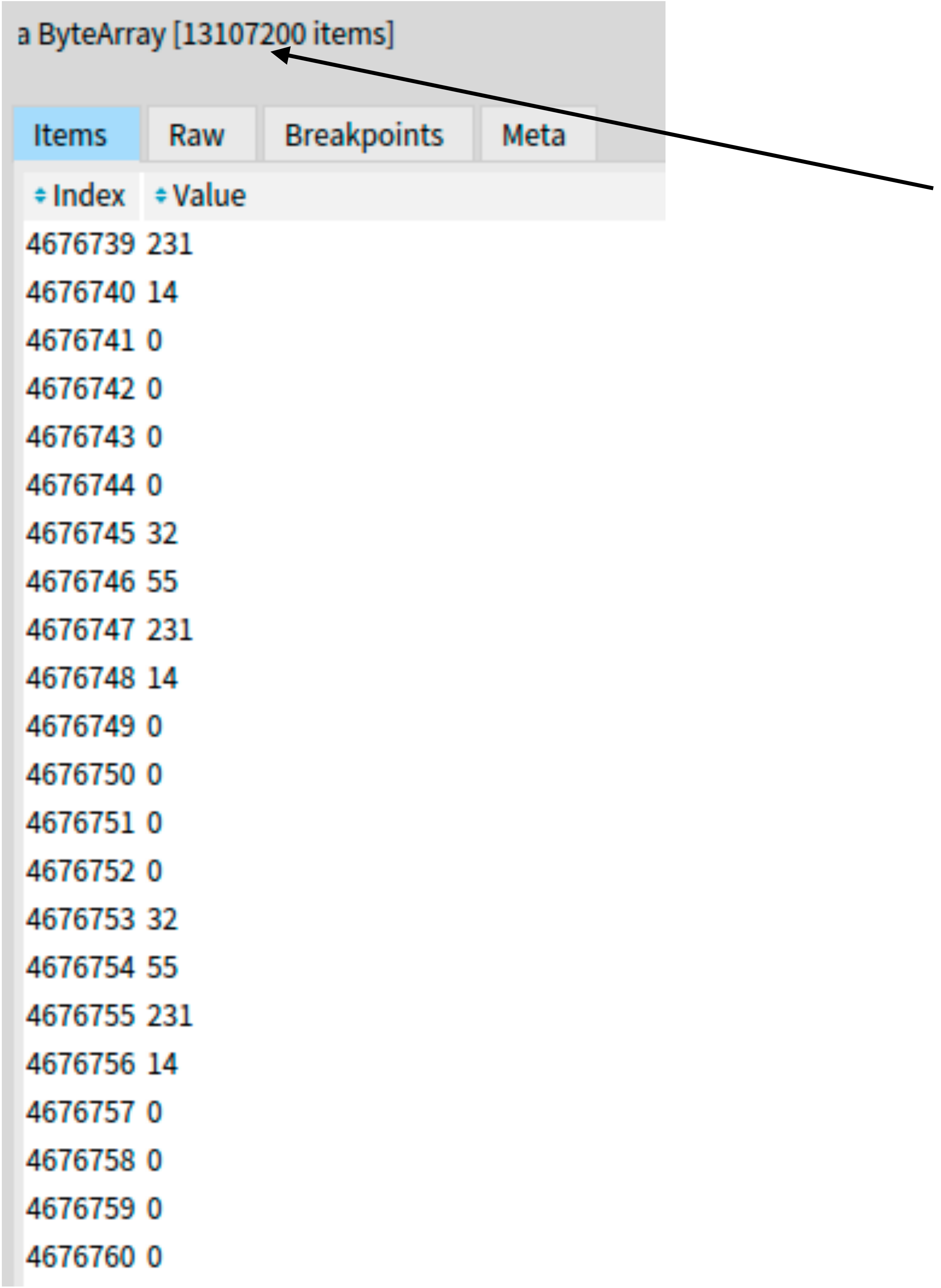
```
scaledByDisplayScaleFactor

	^ self scaledToSize: self extent * self currentWorld displayScaleFactor.
```

Found it !

Let’s do VM level tools !

Let’s find the class Form … But at the VM level …



a ByteArray [13107200 items]

Index	Value
4676739	231
4676740	14
4676741	0
4676742	0
4676743	0
4676744	0
4676745	32
4676746	55
4676747	231
4676748	14
4676749	0
4676750	0
4676751	0
4676752	0
4676753	32
4676754	55
4676755	231
4676756	14
4676757	0
4676758	0
4676759	0
4676760	0

13 107 200 items

Let’s do VM level tools !

With the help of the simulator

```
memory findClassNamed: Form >>> 406749864
```

```
findClassNamed: aClassName
    | classNameIndex classNameOop className |
    memory classTableEntriesDo: [ :aClassOop |
        aClassOop = memory nilOOP
            ifTrue: [ "not a class, nothing to do" ]
            ifFalse: [
                classNameIndex := memory classNameIndexForOop: aClassOop.
                classNameOop := memory fetchPointer: classNameIndex ofObject: address.
                className := memory convertStringOopToStringObject: classNameOop.
                className = aClassName ifTrue: [ ^ aClassOop ]]].
    ^ memory nilOOP
```

Let’s do VM level tools !

Why do I have to code like that ?

- **Ordinary Object Pointers** (OOP)
- Common API
- VM level information

Polyphemus

Introducing LLOOPs

Language level OOPs

Issues

- Ordinary Object Pointers (OOP)
- Common API
- VM level information

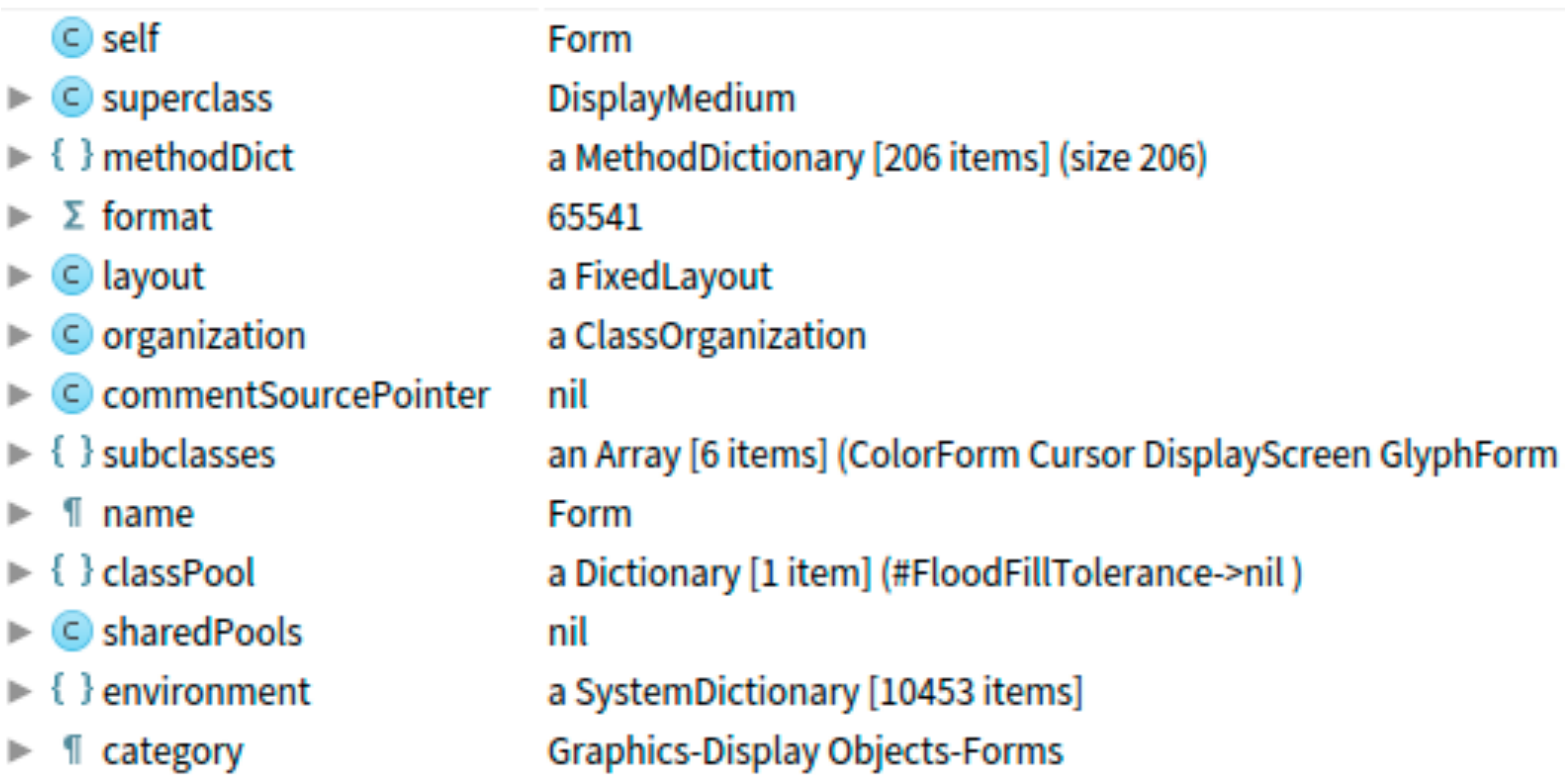
Solutions

- Objects
- Specialized API & Polymorphism
- VM and Language level information

Polyphemus

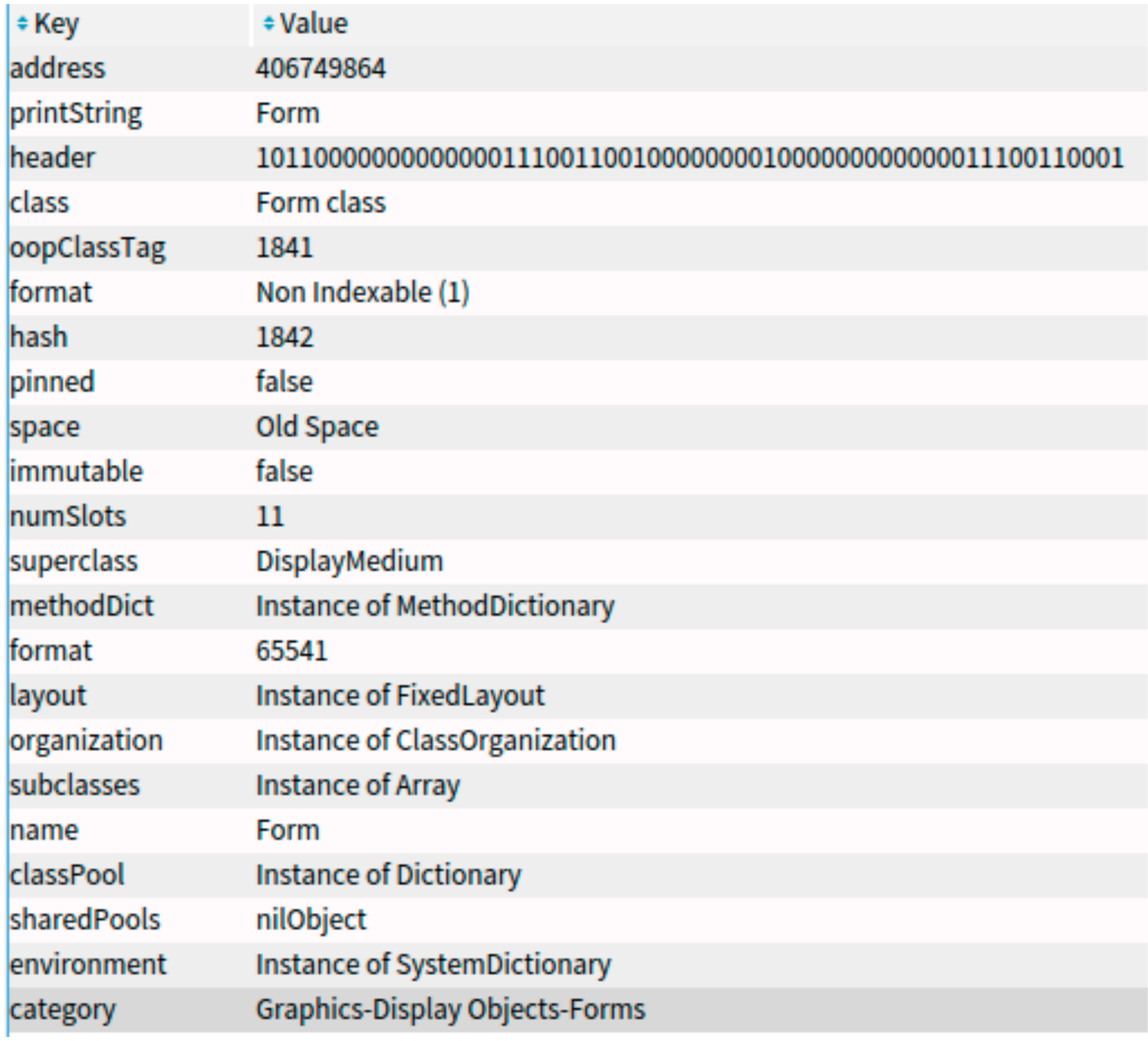
Objects instead of OOPs

Pharo Object



self	Form
superclass	DisplayMedium
methodDict	a MethodDictionary [206 items] (size 206)
format	65541
layout	a FixedLayout
organization	a ClassOrganization
commentSourcePointer	nil
subclasses	an Array [6 items] (ColorForm Cursor DisplayScreen GlyphForm
name	Form
classPool	a Dictionary [1 item] (#FloodFillTolerance->nil)
sharedPools	nil
environment	a SystemDictionary [10453 items]
category	Graphics-Display Objects-Forms

LLOOP



Key	Value
address	406749864
printString	Form
header	1011000000000000011100110010000000010000000000000011100110001
class	Form class
oopClassTag	1841
format	Non Indexable (1)
hash	1842
pinned	false
space	Old Space
immutable	false
numSlots	11
superclass	DisplayMedium
methodDict	Instance of MethodDictionary
format	65541
layout	Instance of FixedLayout
organization	Instance of ClassOrganization
subclasses	Instance of Array
name	Form
classPool	Instance of Dictionary
sharedPools	nilObject
environment	Instance of SystemDictionary
category	Graphics-Display Objects-Forms

Polyphemus

LLOOPs are just the start

- Object specific behavior
- Inspectors
- Memory visualisation

- Many more and more VM level tooling

Polyphemus

Object specific behavior

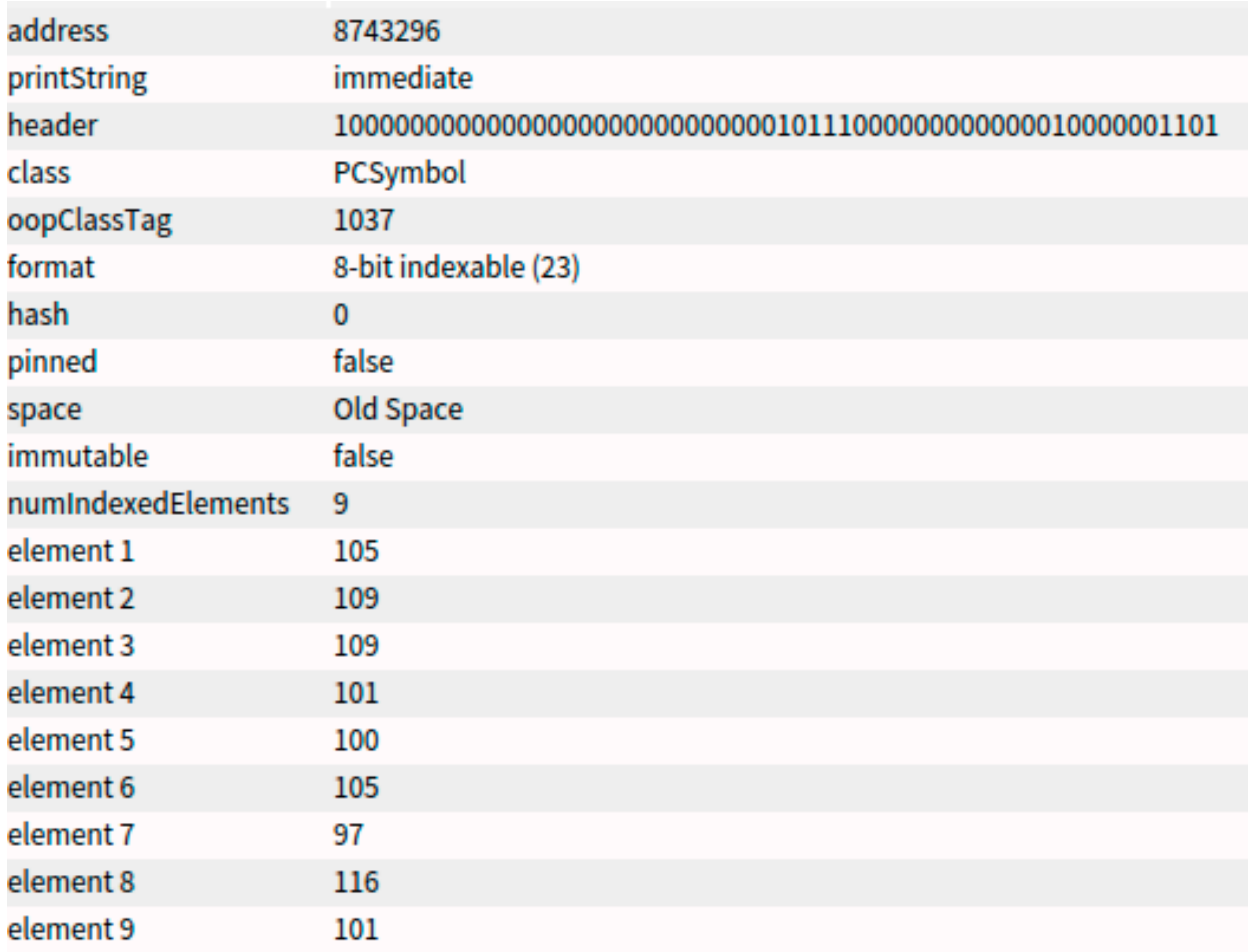
- Classes have subclasses
  formClassOop oopSubclasse >>> 'an Array(DisplayScreen Cursor …)
- A class table page is a VM level object that have an index in the Class Table
  aClassTablePage pageIndexOop
- Indexable Objects are addressed in the same way

```
OOP16BitIndexableObject >> #numElements
    ^ memory num16BitUnitsOf: address
OOP64BitIndexableObject >> #numElements
    ^ memory num64BitUnitsOf: address
```

Polyphemus

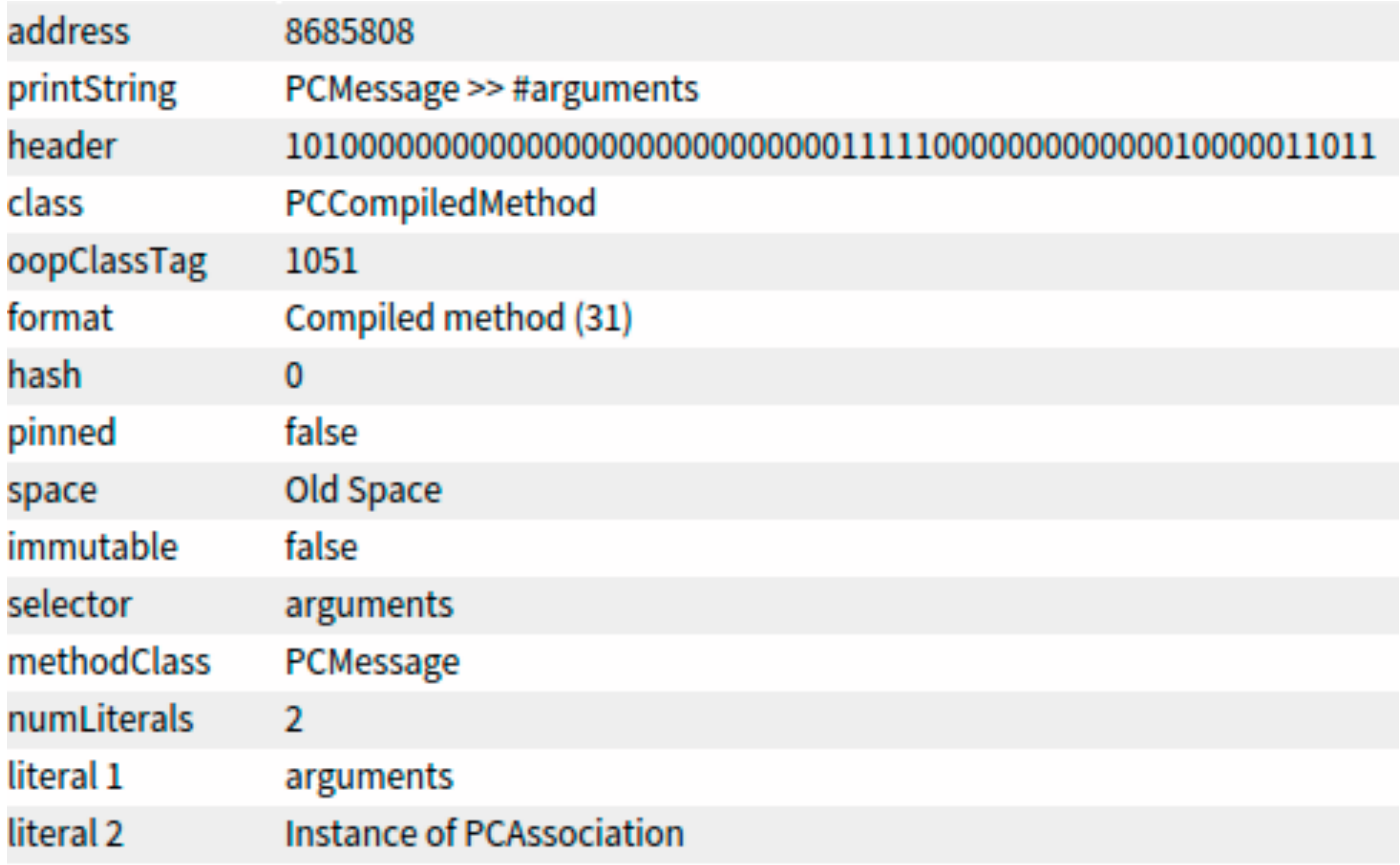
Inspectors

Symbol



address	8743296
printString	immediate
header	1000000000000000000000000000010111000000000000010000001101
class	PCSymbol
oopClassTag	1037
format	8-bit indexable (23)
hash	0
pinned	false
space	Old Space
immutable	false
numIndexedElements	9
element 1	105
element 2	109
element 3	109
element 4	101
element 5	100
element 6	105
element 7	97
element 8	116
element 9	101

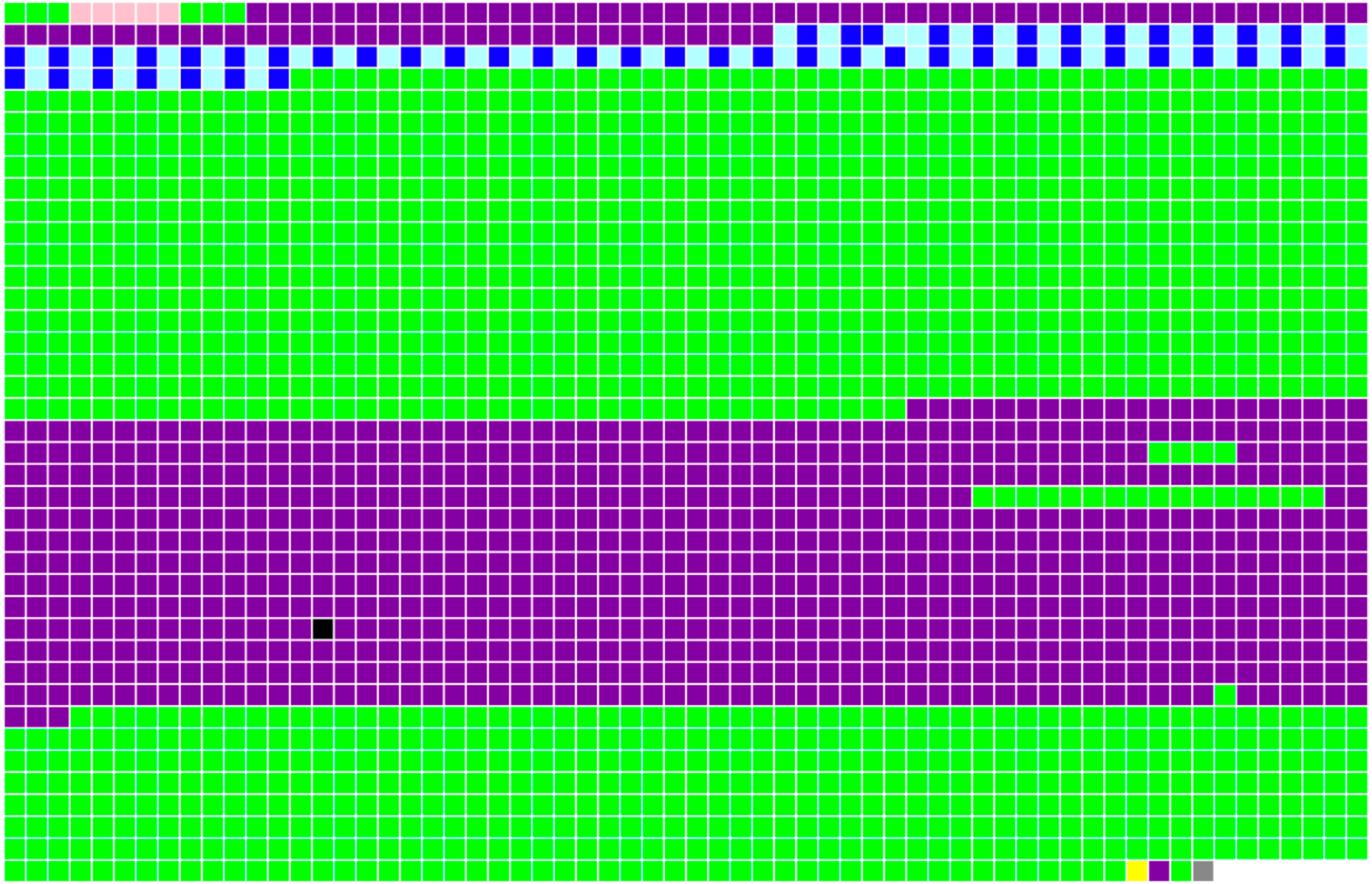
Compiled Method



address	8685808
printString	PCMessage >> #arguments
header	10100000000000000000000000000000011111000000000000010000011011
class	PCCompiledMethod
oopClassTag	1051
format	Compiled method (31)
hash	0
pinned	false
space	Old Space
immutable	false
selector	arguments
methodClass	PCMessage
numLiterals	2
literal 1	arguments
literal 2	Instance of PCAssociation

Polyphemus

Memory visualisation



1 ⬛ pinned object

895 🟪 compiled method

51 🟦 class

5 🟥 special object

1 🟨 context

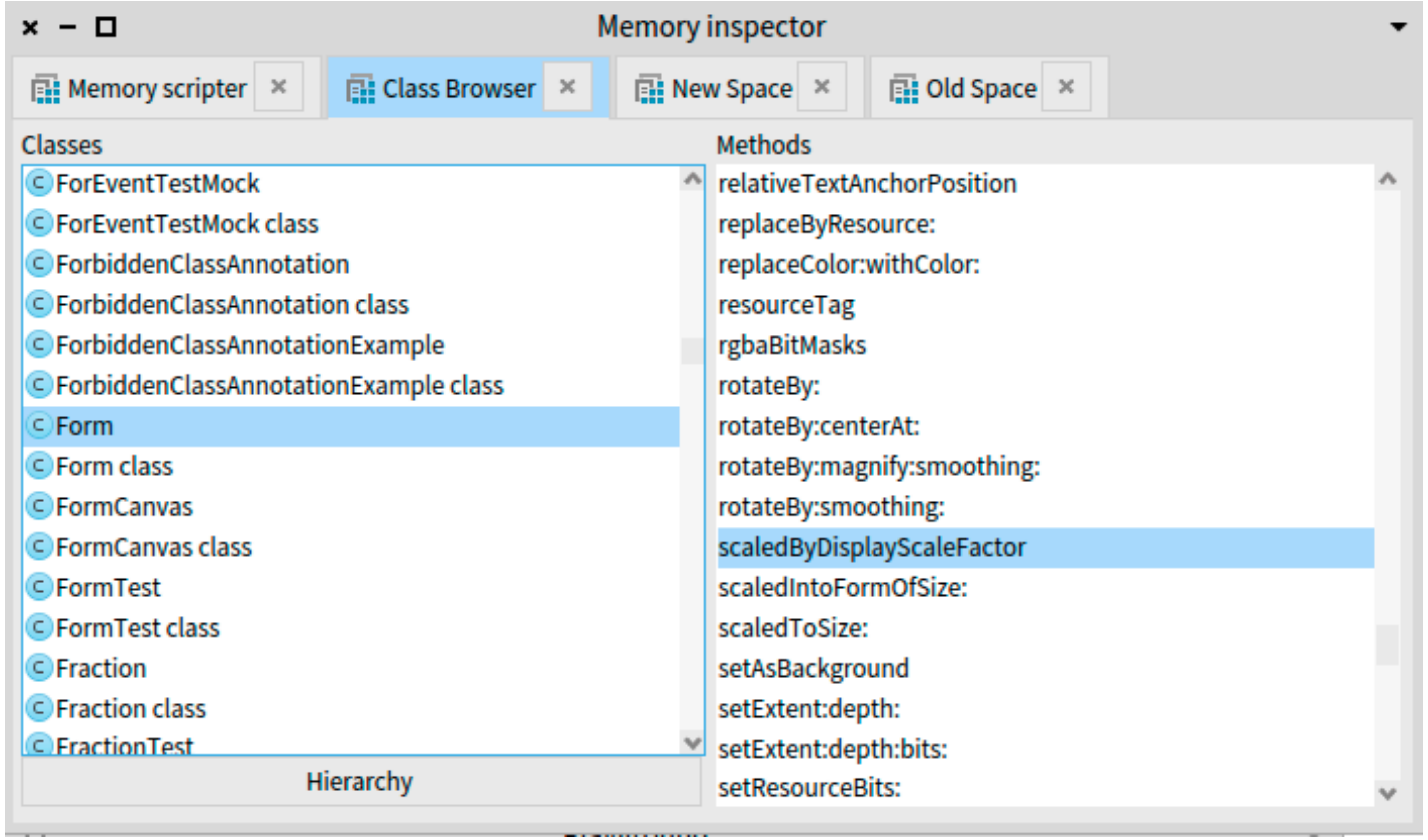
1 ◼ free chunk

1468 🟩 regular object

51 ⬜ metaclass

Polyphemus

Memory visualisation #2



Classes

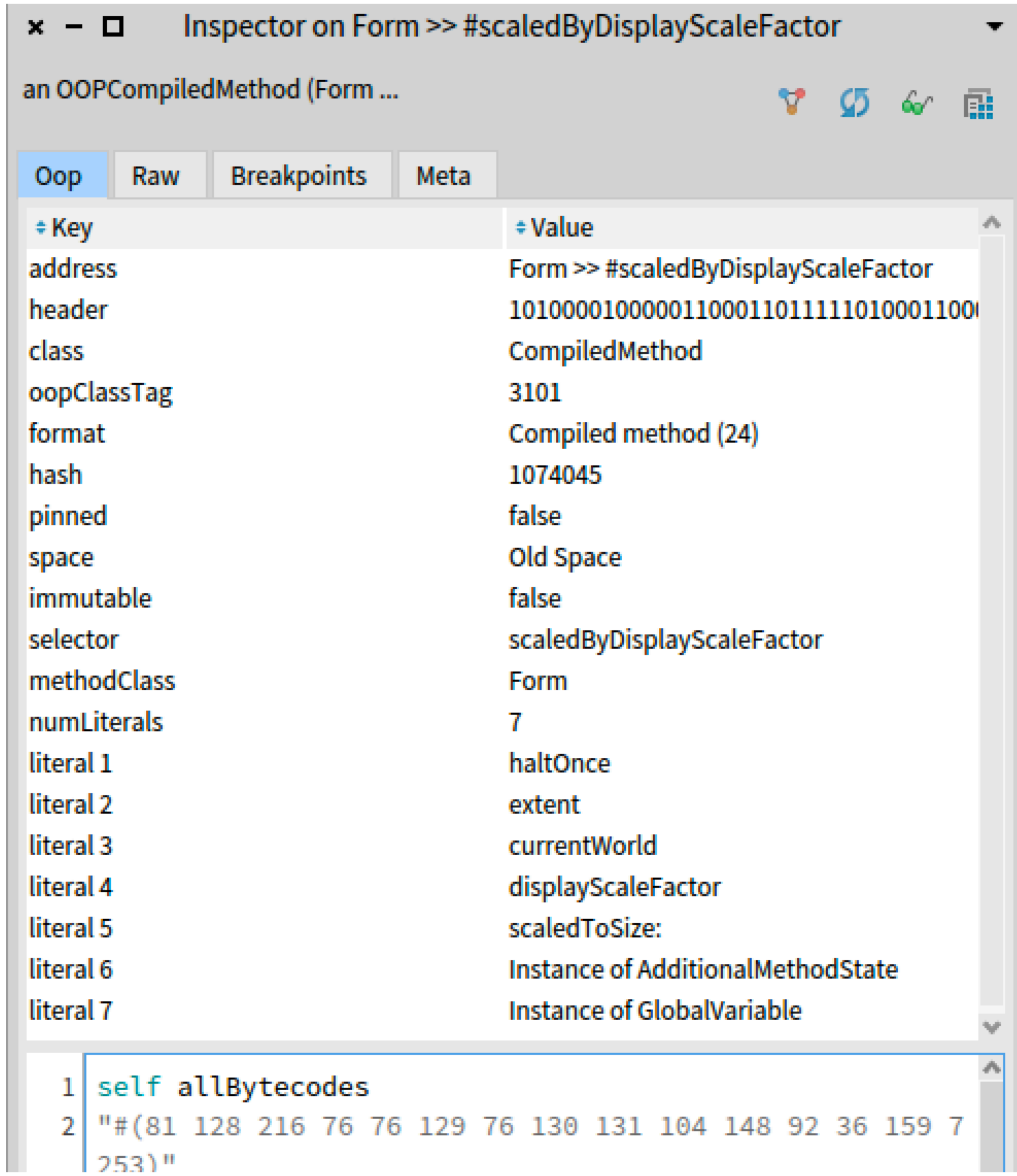
ForEventTestMock
ForEventTestMock class
ForbiddenClassAnnotation
ForbiddenClassAnnotation class
ForbiddenClassAnnotationExample
ForbiddenClassAnnotationExample class
Form
Form class
FormCanvas
FormCanvas class
FormTest
FormTest class
Fraction
Fraction class
FractionTest

Methods

relativeTextAnchorPosition
replaceByResource:
replaceColor:withColor:
resourceTag
rgbaBitMasks
rotateBy:
rotateBy:centerAt:
rotateBy:magnify:smoothing:
rotateBy:smoothing:
scaledByDisplayScaleFactor
scaledIntoFormOfSize:
scaledToSize:
setAsBackground
setExtent:depth:
setExtent:depth:bits:
setResourceBits:

Real World Bug Fix

A Meta-Error fix

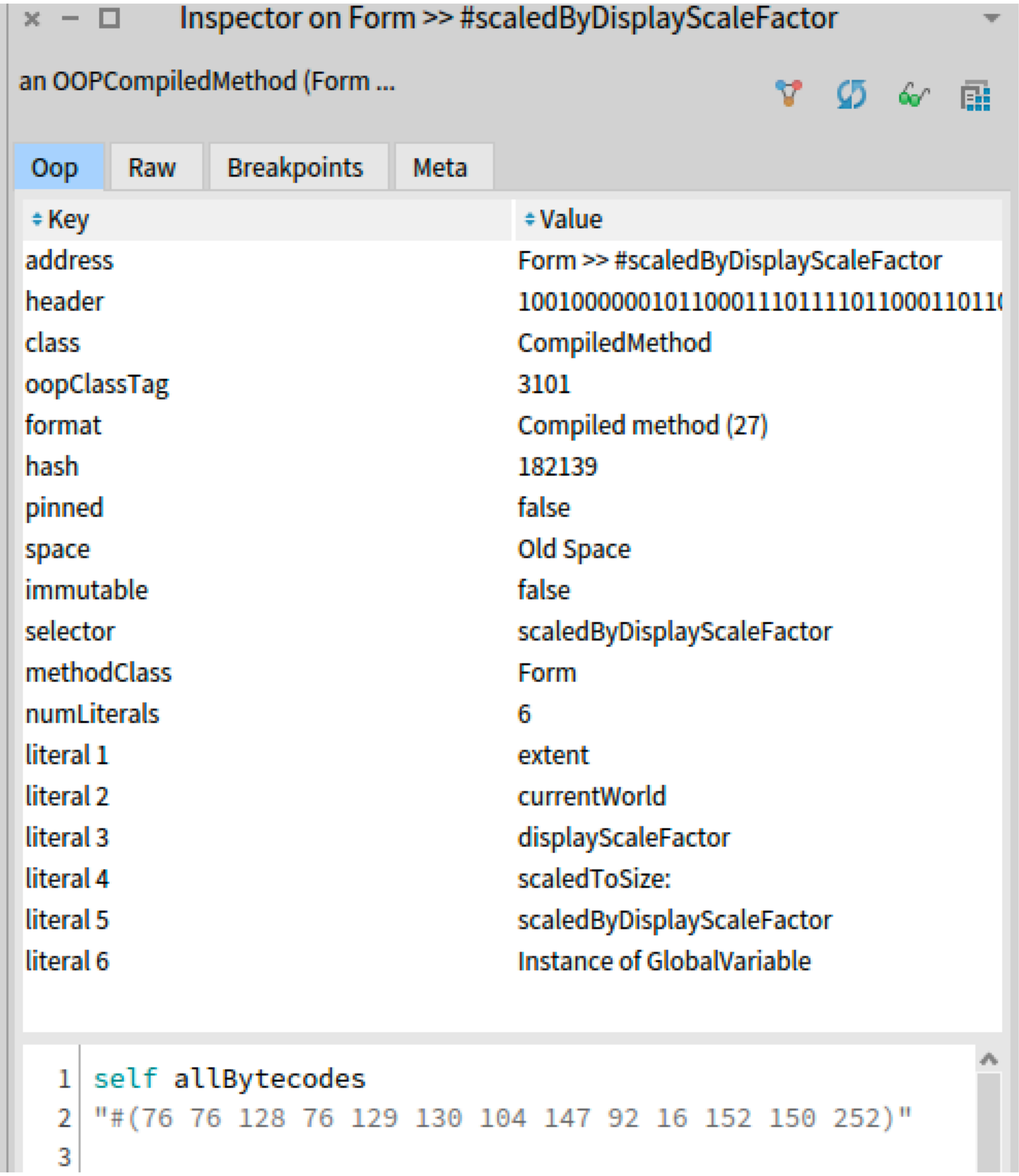


Inspector on Form >> #scaledByDisplayScaleFactor

an OOPCompiledMethod (Form ...

Key	Value
address	Form >> #scaledByDisplayScaleFactor
header	101000010000001100011011111010001100
class	CompiledMethod
oopClassTag	3101
format	Compiled method (24)
hash	1074045
pinned	false
space	Old Space
immutable	false
selector	scaledByDisplayScaleFactor
methodClass	Form
numLiterals	7
literal 1	haltOnce
literal 2	extent
literal 3	currentWorld
literal 4	displayScaleFactor
literal 5	scaledToSize:
literal 6	Instance of AdditionalMethodState
literal 7	Instance of GlobalVariable

```
self allBytecodes
"#(81 128 216 76 76 129 76 130 131 104 148 92 36 159 7
253)"
```



Inspector on Form >> #scaledByDisplayScaleFactor

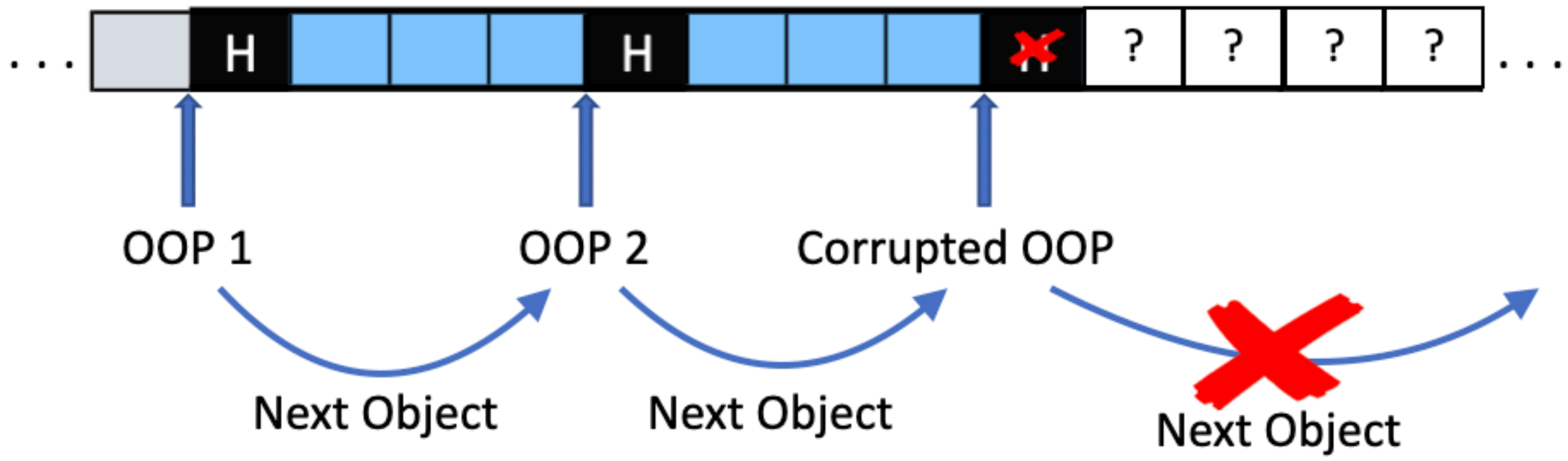
an OOPCompiledMethod (Form ...

Key	Value
address	Form >> #scaledByDisplayScaleFactor
header	1001000000010110001110111101100011011
class	CompiledMethod
oopClassTag	3101
format	Compiled method (27)
hash	182139
pinned	false
space	Old Space
immutable	false
selector	scaledByDisplayScaleFactor
methodClass	Form
numLiterals	6
literal 1	extent
literal 2	currentWorld
literal 3	displayScaleFactor
literal 4	scaledToSize:
literal 5	scaledByDisplayScaleFactor
literal 6	Instance of GlobalVariable

```
self allBytecodes
"#(76 76 128 76 129 130 104 147 92 16 152 150 252)"
```

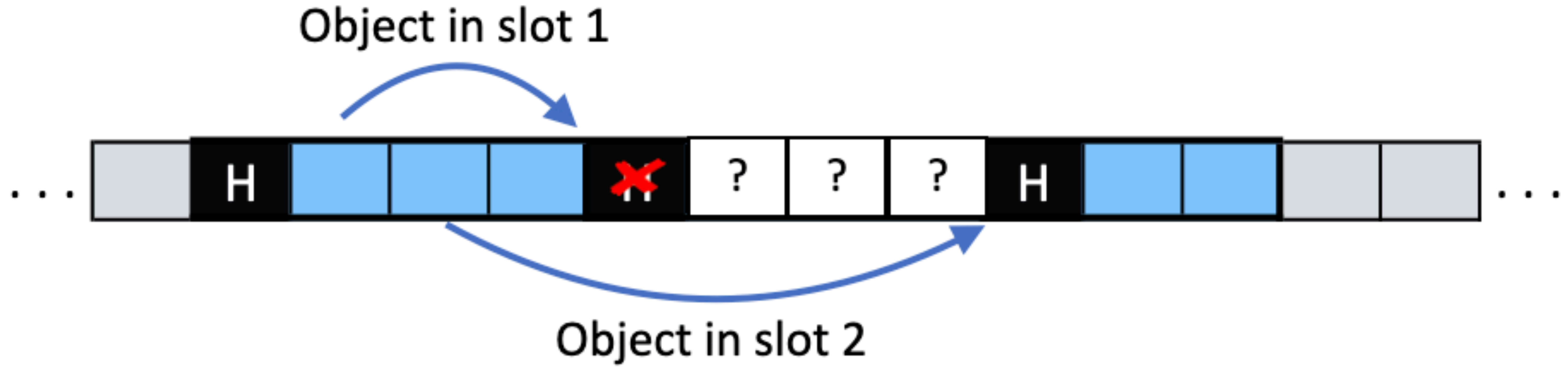
Real World Bug Fix

Iterating the corrupted memory



Real World Bug Fix

Cleansing the memory



Conclusion

https://github.com/hogoww/Polyphemus/

QR code Polyphemus Paper

Tools screenshots

Pierre Misse-Chanabier
pierre.misse-chanabier@inria.fr
github.com/hogoww
Discord tag: hogo#8547