Pharo Virtual Machine News from the Front

P. Tesone - G. Polito - 03/03/2022

Ínría









2022 VM+ Team



ANTARCTICA

Copyright©worldmapblank.com



ARM64 Backend

- ARM64 is now pervasive:
 - New Apple M1
 - Raspberry Pi 4
 - Microsoft Surface Pro X
 - PineBook Pro

- move r1 #1
- move r2 #17

- add r3 r1 r2
- move r1 r3
- ret

JIT compiler IR



checkSmallInt r1 checkSmallInt r2 checkSmallInt r3



Testing & TDDing the VM

- No useful unit tests by ~06/2020
- Large manual testing effort during 2020 while porting to ARM64bits
 - Extended VM simulation with a (TDD compatible) unit testing infrastructure
 - 450+ written tests on the interpreter and the garbage collector*
 - 580+ written tests on the JIT compiler*
 - Parametrisable for 32 and 64bits, ARM32, ARM64, x86, x86-64



* Numbers by 05/2021

Cross-ISA Testing of the Pharo VM. Lessons learned while porting to ARMv8 64bits. Polito et al. MPLR'21





VM Component	Operation	Independent Tests	Variations	Total Execut
	Method Builder	10		20
Test Infrastructure	Stack Builder	18	32 bits / 64 bits	36
	Total	28		56
	Stack Reification	7		14
	Context / Stack Mapping	13		26
	GC Data Structures	13		26
	Unmovable Objects	9		18
	Old Object Garbage Collection	63		126
Object Memory	Young Objects Garbage Collection	38	32 bits / 64 bits	76
	Weak Object Garbage Collection	9		18
	Ephemeron Object Garbage Collec-	19		38
	tion			
	Old Objects FreeSpace Management	85		170
	Memory Structure Preconditions	30		60
	Total	286		572
	Bytecode Tests	43		86
	Method Lookup	15		30
Interpreter	Object Representation	17	32 bits / 64 bits	34
•	Primitives	62		124
	Total	137		274
	Total	451		902



Testing & TDDing the VM

- No useful unit tests by ~06/2020
- Large manual testing effort during 2020 while porting to ARM64bits
 - Extended VM simulation with a (TDD compatible) unit testing infrastructure
 - 450+ written tests on the interpreter and the garbage collector*
 - 580+ written tests on the JIT compiler*
 - Parametrisable for 32 and 64bits, ARM32, ARM64, x86, x86-64





* Numbers by 05/2021

Cross-ISA Testing of the Pharo VM. Lessons learned while porting to ARMv8 64bits. Polito et al. MPLR'21



Automatic Test Generator Interpreter-Guided JIT compiler Testing

- Automatic test generation through interpreter concolic execution
- 2. Bug detection through differential testing





Automatic Test Generator

- Automatic test generation through interpreter concolic execution
- Bug detection through differential testing

- 468 differences found, 91 causes, 6 categories
- Practical: \bullet
 - 4582 tests generated in ~8 minutes
 - 4582 tests run in ~40 seconds



Accepted in PLDI'22 - Top Programming Language Conference



Improving Slang Automatic transformations, simplifications, C AST nodes



/* InterpreterPrimitives>>#primitiveAdd */¬

```
DECL_MAYBE_SQ_GLOBAL_STRUCT; ¬
```

```
integerResult = (stackIntegerValue(1)) + (stackIntegerValue(0));
if (!GIV(primFailCode)) {¬
   if ((((((usqInt) integerResult ) >> 60) + 1) & 15) <= 1) {-</pre>
       longAtput((sp = GIV(stackPointer) + ((2 - 1) * BytesPerWord)), ((((usqInt) int
       GIV(stackPointer) = sp;
           if (!GIV(primFailCode)) {¬
           GIV(primFailCode) = 1;-
```



Tools for Debugging Insights: build your own tools, based on needs, not desires

Examples:

- Machine code debugger
- Bytecode-IR visualization
- Disassembler DSL



× - 🗆

IR Instructions	^	Address
' (PopR 10 13503 810113)'		16r1000000
' (Label 1)'		16r1000004
' (TstCqR 7 10 757D93)'		16r1000008
' (JumpNonZero (Label 2) 20D9063)'		16r100000C
' (MoveMwrR 0 10 22/16 53B03)'		16r1000010
' (AndCqR 4194295/3FFFF7 22/16 no mcode)'		16r1000014
' (JumpNonZero (Label 2) D9663)'		16r1000018
' (MoveMwrR 8 10 10 853503)'		16r100001C
' (Jump (Label 1) FE1FF06F)'		16r1000020
' (Label 2)'		16r1000024
' (MoveMwrR 0 2 23/17 13B83)'		16r1000028
' (Label 3)'		16r100002C
' (TstCqR 7 23/17 7BFD93)'		16r1000030
' (JumpNonZero (Label 4) 20D9063)'		16r1000034
' (MoveMwrR 0 23/17 22/16 BBB03)'		16r1000038
' (AndCqR 4194295/3FFFF7 22/16 no mcode)'		16r100003C
' (JumpNonZero (Label 4) D9663)'		16r1000040
' (MoveMwrR 8 23/17 23/17 8BBB83)'		16r1000044
' (Jump (Label 3) FE1FF06F)'		16r1000048
' (Label 4)'		16r100004C
' (CmpRR 10 23/17 41750DB3)'		16r1000050
' (JumpNonZero (MoveCqR 16856080/1013410 10		16r1000054
' (MoveCqR 16856096/1013420 10 1013537 42050		16r1000058
' (Jump (MoveRMwr 10 0 2 A13023) C0006F)'	v	16r100005C

Jump to

	VM	De	bugger							
ASM	Bytes	٨					^			
ld a0, 0(sp)	#[3 53 1 0]		lr			'16r1001000'		SP	16r1002FE8	16
addi sp, sp, 8	#[19 1 129 0]	рс			'16r1000'			16r1002FF0	16
andi s11, a0,	#[147 125 1	1	sp			'16r1002FE8'			16r1002FF8	16
bnez s11, 32	#[99 144 13	:	fp			'16r1003000'		FP	16r1003000	16
ld s6, 0(a0)	#[3 59 5 0]		x0	zero)	'16r0'			16r1003008	16
lui t0, 1024	#[183 2 64 0]	x1	ra		'16r1001000'			16r1003010	16
addiw t0, t0,	·#[155 130 1	1	x2	sp	sp	'16r1002FE8'			16r1003018	16
and s6, s6, t0	#[51 123 91	(х3	gp		'16r0'			16r1003020	16
bnez s11, 12	#[99 150 13	(x4	tp		'16r0'			16r1003028	16
ld a0, 8(a0)	#[3 53 133 0]	x5	t0	ip1	'16r0'			16r1003030	16
j-32	#[111 240 3	1	x6	t1	ip2	'16r0'			16r1003038	16
ld s7, 0(sp)	#[131 59 1 0]	x7	t2		'16r0'			16r1003040	16
andi s11, s7, i	1#[147 253 1	2	x8	s0(fj	p) fp	'16r1003000'			16r1003048	16
bnez s11, 32	#[99 144 13	:	x9	s1		'16r0'			16r1003050	16
ld s6, 0(s7)	#[3 187 11 0]	x10	a0	arg0	'16r0'			16r1003058	16
lui t0, 1024	#[183 2 64 0]	x11	al	arg1	'16r0'			16r1003060	16
addiw t0, t0,	·#[155 130 1	1	x12	a2	carg0	'16r0'			16r1003068	16
and s6, s6, t0	#[51 123 91	(x13	a3	carg1	'16r0'			16r1003070	16
bnez s11, 12	#[99 150 13	(x14	a4	carg2	'16r0'			16r1003078	16
ld s7, 8(s7)	#[131 187 1	3	x15	a5	carg3	'16r0'			16r1003080	16
j-32	#[111 240 3	1	x16	a6		'16r0'			16r1003088	16
sub s11, a0, s	#[179 13 11	7	x19	s3	extra1	'16r0'			16r1003090	16
bnez s11, 16	#[99 152 13	(x20	s4	extra2	'16r0'			16r1003098	16
lui a0, 4115	#[55 53 1 1]	v	x22	s6	temp	'16r0'	~		16r10030A0	16



Improvements: Clean Up

- V3 Support
- Old Memory Format
- Old Block Closures
- Dead Code
- ~ 65KLOC

Improvements: Sockets

- Unified Implementation in all Platforms
- Better Async Support
- Unix Sockets (Under Work)
- IPv6 Addresses (Under Work)

Improvements: Serial Port FFI

- Pure FFI implementation
- Migrating Plugins to FFI

• Working in all Platforms (Unix / Windows / OSX)

Improvements: RISCV64 Ongoing Port

- Currently under development: Real HW testing stage
- Taking advantage of our harness test suite.
- Improving tests and scenarios

- Future work on: Hardware-based security enforcement

Collaboration with Q. Ducasse, P. Cortret, L. Lagadec from ENSTA Bretagne





Improvements: Open Build Service Better Support for Linux Distributions

	Arch	Deb	ian_10	Debian_9.0	Deb	oian_Testing	Fedora_3	1	Fedora_32	Fedora_	33	Rasp	bian_10	Raspbia	n_9.0
Λ	, 🛤 x86	_64 🏎 🛼	86_64∿	🔜 x86_64∿	U	a x86_64 ↑↓	🛼 x86_6	54∿	😝 x86_64∿	🛼 x86_	64 U	🛼 aarch64	↓ 🛼 x86_64↓	🗦 aarch64\/	, x86_64∜
libffi7		suc	ceeded	succeeded			succeed	ed	succeeded	succee	ded	succeeded	succeeded	succeeded	succeeded
libgit2-1		suc	ceeded			failed									
pharo9	faile	d suc	ceeded	failed		failed	failed		failed	faile	d	succeeded	succeeded	failed	failed
pharo9-ui	succee	eded suc	ceeded	succeeded		failed	succeed	ed	succeeded	succee	ded		succeeded		succeeded
		k													
	Raspbia	n_9.0	oper	nSUSE_Leap_15	5.1	openSUSE_Le	ap_15.2	ope	enSUSE_Tumble	eweed	xUbu	untu_18.04	xUbuntu_19.04	xUbunt	u_20.04
↑ ↓	arch64∜	🛼 x86_6	\$↓	🛼 x86_64	↑↓	🛼 x86_(64 îų		🛼 x86_64	ŤΨ		x86_64 🛝	🛼 x86_64 🛝	aarch64	x86_64 ∜
libffi7	ceeded	succeede	d	succeeded		succeed	bed		succeeded	ł	s	ucceeded	succeeded	succeeded	succeeded
libgit2-1				succeeded		succeed	bed				s	ucceeded	succeeded		succeeded
pharo9	failed	failed		failed		failed	I		failed			failed	succeeded	succeeded	succeeded
pharo9-ui		succeede	d	succeeded		succeed	ded		succeeded	k	s	ucceeded	succeeded		succeeded

	Arch	Debiar	n_10	Debian_9.0	Debi	an_Testing	Fedora_3	81	Fedora_32	Fedora_	33	Raspl	pian_10	Raspbia	n_9.0
↑ ↓	🛼 x86_	_64⊎ 🛼 x86	6_64∿			x86_64 ↑↓	🛼 x86_6	54∿	,∋ x86_64⊍	🛼 x86	64 ∿	🛤 aarch64	↓ 🛼 x86_64∜	🔒 aarch64\/	,∋ x86_64∜
libffi7		succe	eded	succeeded			succeed	ed	succeeded	succee	ded	succeeded	succeeded	succeeded	succeeded
libgit2-1		succe	eded			failed									
pharo9	faile	d succe	eded	failed		failed	failed		failed	faile	d	succeeded	succeeded	failed	failed
pharo9-ui	succee	ded succe	eded	succeeded		failed	succeed	ed	succeeded	succee	ded		succeeded		succeeded
	Raspbia	n_9.0	open	SUSE_Leap_15	i.1 c	ppenSUSE_Le	ap_15.2	ope	nSUSE_Tumble	eweed	xUb	untu_18.04	xUbuntu_19.04	xUbunt	u_20.04
€	arch64∿	🛼 x86_64⊍	1	x86_64	ŤΨ	🛼 x86_(64 îų		🛼 x86_64	心		x86_64 🛝	🛼 x86_64 🛝	🛼 aarch64	x86_64 U
libffi7	ceeded:	succeeded		succeeded		succeed	bed		succeeded	l	s	ucceeded	succeeded	succeeded	succeeded
libgit2-1				succeeded		succeed	bed				s	ucceeded	succeeded		succeeded
pharo9	failed	failed		failed		failed	I		failed			failed	succeeded	succeeded	succeeded
pharo9-ui		succeeded		succeeded		succeed	ded		succeeded	l	S	ucceeded	succeeded		succeeded



Multiple Architectures

Supporting system packagings

Initial targets:

- Arch / Manjaro
- Debian
- Fedora
- Raspbian
- Ubuntu
- openSuse

Building using existing system libraries



Improvements: Visual Studio Support Building & Debugging

図 Eile Edit View Git Project Build	Debug Test Analyze Tools Extensions Window	Hel
Debu	ig ~ ARM64 ~ ▶ Continue ~ 🎜 🙆	
Process: [0x2730] PharoConsole.exe 👻 📧 L	fecycle Events * Thread:	7
Registers X0 = 0000000135715120 X1 = 00000000000000 X6 = 0000016F7520AA28 X7 = 0000000000000 X12 = 00000037C9E81000 X13 = 00000000000 X18 = 00000000000000 X19 = 00000037CA X24 = 00000000000000 X25 = 00000000000 LR = 00007FF987993CE8 SP = 00000037CA0D	09 X2 = 00007FF9755F8830 X3 = 00000000000000007 X4 0000 X8 = 0000000000000000 X9 = 000000000000000	= K10 B30 109 000
Disassembly soWin32Directory c Filed	ttributesDlugin c R X straigh pharo h aioW	in c
FileAttributesPlugin	(Global Scope)	in inc
579 { 580 sqInt attributeNumber; 581 fapath faPath; () C:\Users\Ise\Downloads\tffi\tffi\tffi.1.image ; Pharo Tools System	g Windows Help	_
× – □ Play	yground ~	
Doit Publish Bindings Pages	× – 🗆 UndefinedO	bje
1	Models ^ V C ProtoObject	i
	Numbers V C Object	🗆) e
	Pragmas C False	ike D a
100.5	Processes © True	b
Find	Filter	c
×=	● All Packages ○ Scoped View ● Flat ○ Hier. ● In	st. s
	? Comment × © UndefinedObjec× 🙏 UML-C	las
Line: 1:1	Object subclass: #UndefinedObject instanceVariableNames: '' classVariableNames: '' package: 'Kernel-Objects'	
Playground UndefinedObject	A Excessive number of methods ¥ 7	
		_
Autos Locals Watch 1 Find Symbol Results		te
	Call Stack Breakpoin	11.5
🗇 Ready	Call Stack Breakpoir	its.



MSVC - No cygwin



Improvements: Windows ARM



			– ø ×	
Test Puppe	or	-		
274	er 4 ran, 270 passed, 0 skipped, 3 expe liures, 1 error, 0 passed unexpected	cted failures, 0		
Cr	mdMenu>>asSpMenuPresente	r	~	
ic nic-Tesi Filter	Activator Menultem Me	de asSpMenuPrese er-Spec2-Compatil on	enter	MSVC - No
View • Flat O Hier. • I	Inst. side O Class side 🔍 Metho	ods O Vars <u>Class refs.</u> Q Impleme	ntors 🔍 Senders	
	CmdMenu activationStrategyClass rootGroup activationStrategyClass activationStrategyClass: asSpMenuPresenter buildBrowserNotebookActions buildBrowserTabActions buildBrowserToolbar: buildCommandItemInContextactivatingBy: buildContextMenuFor:		Presp	
× - 0	System Rep	orter	•	
Image Parameters Image Parameters Image Sources MC Repositories MC Working Copies VM General VM Options VM Modules VM Parameters VM Stats OS OS Environment OS Details	rating System/Hardware 22 Windows-ARM64 ARM64			
 	^	© 👝 📾 🦟 ປ× 🖋 ເ	NG 15:08 UK 10/12/2020	



Improvements: Raspbian 32/64 bits

💈 Pharo Tools

System Debugging Windows Help

× - 🗆	System Reporter	
Image Image Parameters	Operating System Environme	nt
iniage Farameters		
Image Sources	COLORTERM=truecolor	
MC Repositories	DBUS_SESSION_BUS_ADDRE	× - 🗆
MC Working Copies	/session-ef2f7aa707634b98/t	
VM General	DESKTOP_SESSION=LXDE-pi	Do it Pul
VM Options	DISPLAY=:1.0	1 1 ti
VM Modules	DISPLAYNUM=1	
VM Parameters	GPG_AGENT_INFO=/run/user	
VM Stats	HOME=/home/pi	
OS	HOSTNAME=raspberrypi	
OS Environment	LANG=en_GB.UTF-8	
OS Details	LC_CTYPE=UTF-8	
	LC_TERMINAL=iTerm2	
	LC_TERMINAL_VERSION=3.3.	
	LD_LIBRARY_PATH=/usr/lib/a	
	b:/lib/aarch64-linux-gnu:/lib:	
	r/lib:	
	LOGNAME=pi	
	LS_COLORS=rs=0:di=01;34:ln	
	35:do=01;35:bd=40;33;01:cd=	
	=37;41:sg=30;43:ca=30;41:tw	
	1;32:*.tar=01;31:*.tgz=01;31:*	Line: 1:1
	1;31:*.lha=01;31:*.lz4=01;31:*	,
	01;31:*.txz=01;31:*.tzo=01;31:	*.t7z=01;31:
	;31:*.dz=01;31:*.gz=01;31:*.lrz	=01;31:*.lz=
	.xz=01;31:.zst=01;31:*.tzst=0)1;31:*.bz2=
	.tbz=01;31:*.tbz2=01;31:*.tz=0)1;31:*.deb=
	:*.jar=01;31:*.war=01;31:*.ear	=01;31:*.sar





Back to the Future Objectives for 2022





Permanent Space Problem

- Many permanent objects
- They have references from/to other objects
- We are traversing them to GC
- E.g., Classes, Methods, Literals, Resources

Generates Long Pauses (GC/ Saves/Loads)

Permanent Space Our Solution

- New Object Space for permanent Objects
- Minimise or Eliminate GC passes
- Persisting them through executions

Permanent Space Our Solution

- New Object Space for permanent Objects
- Minimise or Eliminate GC passes
- Persisting them through executions

We need to put them in a separate place

New Image Format **Problem**

- Current Image format only support a single object space
- No extensible: not new metadata nor new data
- Cannot be Memory Mapped (it is modified before save/load)
- Requires to discard all state of the running VM (slow saves)

New Image Format **Problem**

- Current Image format only support a single object space
- No extensible: not new metadata nor new data
- Cannot be Memory Mapped (it is modified before save/load)
- Requires to discard all state of the running VM (slow saves)

Slow and Restricting **PermSpace**

New Image Format **Our Solution**

- New Image format based in directories / bundles
- Many Elements of data and metadata
- Metadata en User & Machine readable format (STON?)
- Extensible format

Fast Snapshots / Loading **Based on PermSpace & Image Format**

- Memory Mapped Image
- Shareable State
- Saving / Loading Warm State of the VM

Next Objectives

Permanent Space New Image Format Faster Startup / Saving

- ARM64, RISCV64, Slang...
- Lots of Tests!
- Integration: Sockets, serial
- Visual Studio, Open Build Service

Ephemerons

Speculative Compilation

@pharoproject pharo.org consortium-adm@pharo.org discord.gg/QewZMZa thepharo.dev

