Методы трансляции машинного кода из x86 в ARM

Студент: Нитенко М.Ю., ИУ7-73Б
Научный руководитель: Оленев А. А.

Москва, 2021 г.

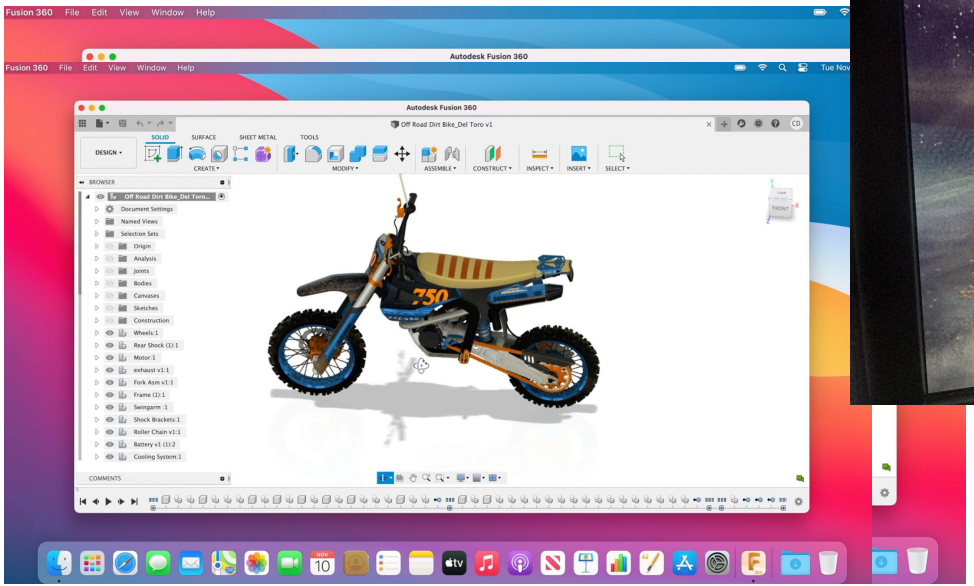
Цель научно-исследовательской работы

Цель данной работы – провести обзор методов применяемых в трансляции машинного кода на x86 в машинный код архитектуры ARM.

Задачи работы:

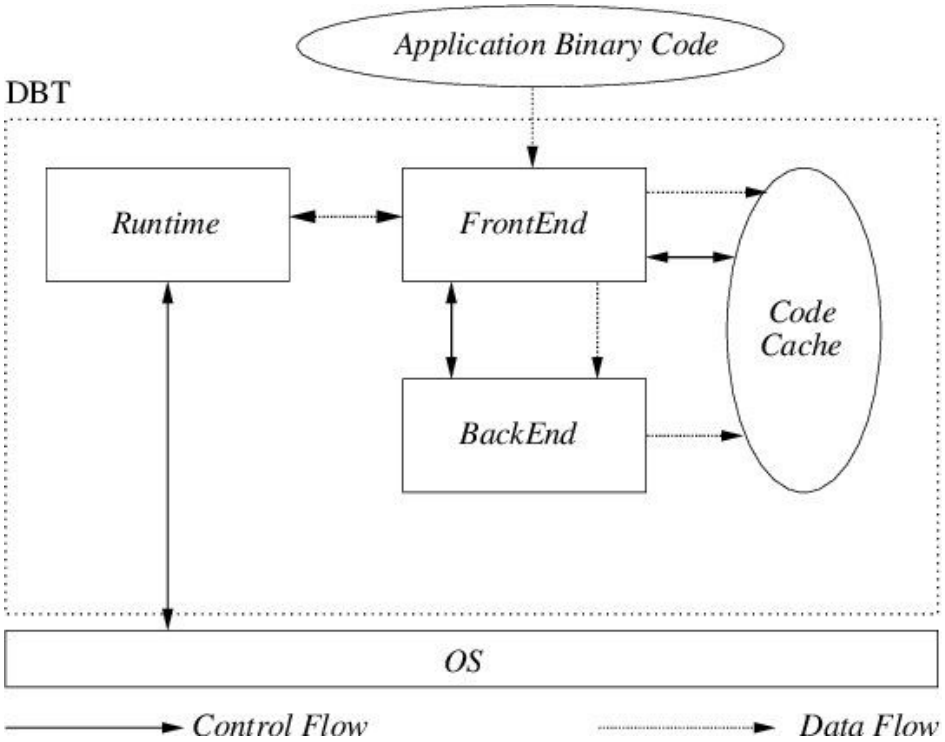
- проанализировать существующие подходы к трансляции;
- проанализировать существующие оптимизации трансляции.

Трансляция


Fusion 360
File
Edit
View
Window
Help
Autodesk Fusion 360
Off Road Dirt Bike_Del Toro v1
DESIGN
SOLID
SURFACE
SHEET METAL
TOOLS
CREATE
MODIFY
ASSEMBLE
CONSTRUCT
INSPECT
INSERT
SELECT
BROWSER
COMMENTS


STELLARIS
Stellaris 3.1 'Lem'
Greetings!
The Curiodians have arrived!
Close
FEELWORLD

Трансляция

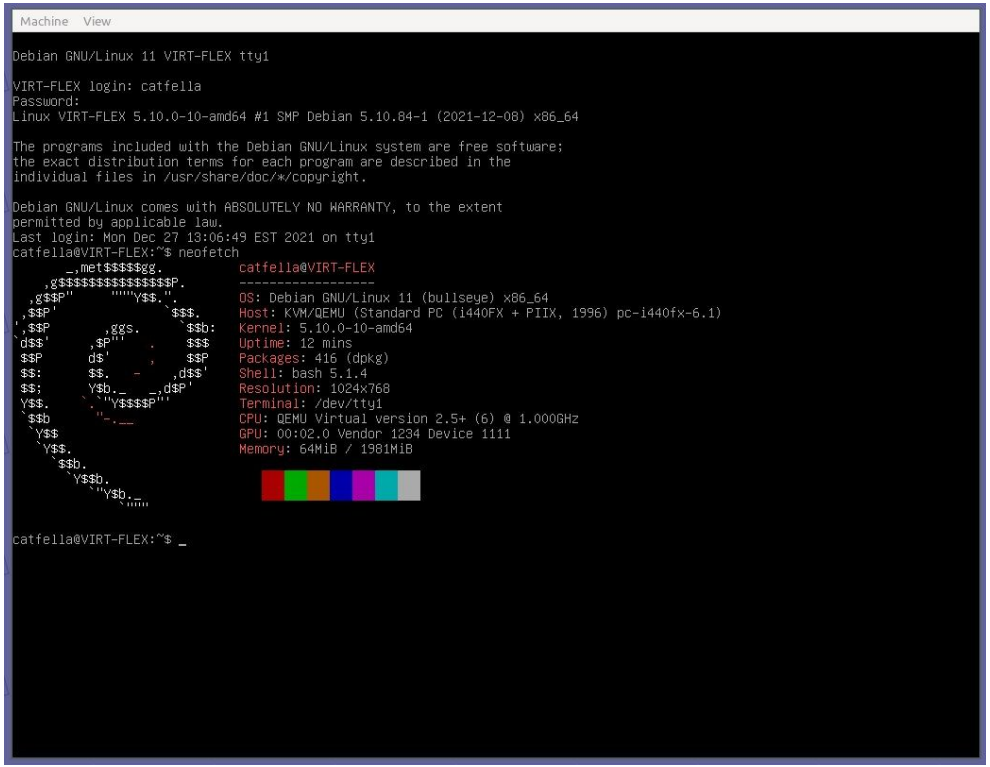

Application Binary Code
DBT
Runtime
FrontEnd
Code Cache
BackEnd
OS
Control Flow
Data Flow

QEMU

```
catfella㉿» LD_LIBRARY_PATH="/home/catfella/libx86/" ~/sd/qemu/build/qemu-x86_64
 ~/Telegram\ Desktop/nbench_x86_O3

BYTEmark* Native Mode Benchmark ver. 2 (10/95)
Index-split by Andrew D. Balsa (11/97)
Linux/Unix* port by Uwe F. Mayer (12/96,11/97)

TEST                : Iterations/sec.  : Old Index   : New Index
                    :                  : Pentium 90* : AMD K6/233*
--------------------:------------------:------------:-----------
NUMERIC SORT        :          295.87  :       7.59  :      2.49
STRING SORT         :          57.319  :      25.61  :      3.96
BITFIELD            :      9.2194e+07  :      15.81  :      3.30
FP EMULATION        :          102.86  :      49.36  :     11.39
FOURIER             :          1950.1  :       2.22  :      1.25
ASSIGNMENT          :          7.2246  :      27.49  :      7.13
IDEA                :          1230.4  :      18.82  :      5.59
HUFFMAN             :          626.46  :      17.37  :      5.55
LU DECOMPOSITION    :           91.67  :     147.26  :     61.94
==========================ORIGINAL BYTEMARK RESULTS==========================
INTEGER INDEX       : 20.181
FLOATING-POINT INDEX: 6.886
Baseline (MSDOS*)   : Pentium* 90, 256 KB L2-cache, Watcom* compiler 10.0
============================LINUX DATA BELOW============================
CPU                 : 6 CPU Cortex-A53
L2 Cache            :
OS                  : Linux 5.15.11-1-MANJARO-ARM
C compiler          : gcc version 11.2.0 (Ubuntu 11.2.0-7ubuntu2)
libc                :
MEMORY INDEX        : 4.537
INTEGER INDEX       : 5.446
FLOATING-POINT INDEX: 4.257
Baseline (LINUX)    : AMD K6/233*, 512 KB L2-cache, gcc 2.7.2.3, libc-5.4.38
* Trademarks are property of their respective holder.
catfella㉿»                                                        [21:21:04]
```



box64

```
catfella➜~» BOX64_LD_LIBRARY_PATH=/home/catfella/libx86 ./sd/box64/build/box64 T
elegram\ Desktop/nbench_x86_O3
Dynarec for ARM64, with extension: ASIMD AES CRC32 PMULL PageSize:4096
Box64 with Dynarec v0.1.6 e6e9fae built on Dec 15 2021 11:37:41
BOX64_LD_LIBRARY_PATH: /home/catfella/libx86/
Using default BOX64_PATH: ./:bin/
Counted 48 Env var
Looking for Telegram Desktop/nbench_x86_O3
Using native(wrapped) libm.so.6
Using native(wrapped) libc.so.6
Using native(wrapped) ld-linux-x86-64.so.2
Using native(wrapped) libpthread.so.0
Using native(wrapped) librt.so.1

BYTEmark* Native Mode Benchmark ver. 2 (10/95)
Index-split by Andrew D. Balsa (11/97)
Linux/Unix* port by Uwe F. Mayer (12/96,11/97)

TEST                : Iterations/sec.  : Old Index   : New Index
                    :                  : Pentium 90* : AMD K6/233*
--------------------:------------------:-------------:------------
NUMERIC SORT        :          372.42  :        9.55 :       3.14
STRING SORT         :          178.12  :       79.59 :      12.32
BITFIELD            :      1.5937e+08  :       27.34 :       5.71
FP EMULATION        :          111.26  :       53.39 :      12.32
FOURIER             :           33841  :       38.49 :      21.62
ASSIGNMENT          :          6.9666  :       26.51 :       6.88
IDEA                :          1873.4  :       28.65 :       8.51
HUFFMAN             :          801.12  :       22.22 :       7.09
LU DECOMPOSITION    :          365.62  :      587.34 :     247.06
==========================ORIGINAL BYTEMARK RESULTS==========================
INTEGER INDEX       : 29.341
FLOATING-POINT INDEX: 28.274
Baseline (MSDOS*)   : Pentium* 90, 256 KB L2-cache, Watcom* compiler 10.0
============================LINUX DATA BELOW============================
CPU                 : 6 CPU GenuineIntel Intel Pentium IV @ 1.416GHz 1416MHz
L2 Cache            : 4096
OS                  : Linux 5.15.11-1-MANJARO-ARM
C compiler          : gcc version 11.2.0 (Ubuntu 11.2.0-7ubuntu2)
libc                :
MEMORY INDEX        : 7.850
INTEGER INDEX       : 6.949
FLOATING-POINT INDEX: 17.480
Baseline (LINUX)    : AMD K6/233*, 512 KB L2-cache, gcc 2.7.2.3, libc-5.4.38
* Trademarks are property of their respective holder.
catfella➜~»                                                        [21:27:46]
```

FEX

```
catfella➜~» ~/sd/FEX/Build/Bin/FEXLoader -R ~/.fex-emu/RootFS/Ubuntu_2110 --thun
kguestlibs=/home/catfella/libx86 ~/Telegram\ Desktop/nbench_x86_03

BYTEmark* Native Mode Benchmark ver. 2 (10/95)
Index-split by Andrew D. Balsa (11/97)
Linux/Unix* port by Uwe F. Mayer (12/96,11/97)

TEST                : Iterations/sec.  : Old Index   : New Index
                    :                  : Pentium 90* : AMD K6/233*
--------------------:------------------:-------------:------------
NUMERIC SORT        :          223.51  :       5.73  :       1.88
STRING SORT         :          24.961  :      11.15  :       1.73
BITFIELD            :      5.6232e+07  :       9.65  :       2.01
FP EMULATION        :          41.876  :      20.09  :       4.64
FOURIER             :          9680.5  :      11.01  :       6.18
ASSIGNMENT          :          10.057  :      38.27  :       9.93
IDEA                :          2057.4  :      31.47  :       9.34
HUFFMAN             :          573.74  :      15.91  :       5.08
LU DECOMPOSITION    :          281.51  :     452.22  :     190.22
========================ORIGINAL BYTEMARK RESULTS==========================
INTEGER INDEX       : 15.721
FLOATING-POINT INDEX: 17.075
Baseline (MSDOS*)   : Pentium* 90, 256 KB L2-cache, Watcom* compiler 10.0
============================LINUX DATA BELOW================================
CPU                 : GenuineIntel FEX-2112 3000MHz
L2 Cache            : 512 KB
OS                  : Linux 5.15.11
C compiler          : gcc version 11.2.0 (Ubuntu 11.2.0-7ubuntu2)
libc                :
MEMORY INDEX        : 3.256
INTEGER INDEX       : 4.512
FLOATING-POINT INDEX: 10.556
Baseline (LINUX)    : AMD K6/233*, 512 KB L2-cache, gcc 2.7.2.3, libc-5.4.38
* Trademarks are property of their respective holder.
catfella➜~»                                                        [21:50:59]
```

SSA

(%%ssa3) CodeBlock %%ssa169, %%ssa173, %%ssa4

(%%ssa169) BeginBlock %ssa3

%ssa170 i64 = Constant 0x41a9e1

(%%ssa171) StoreContext %ssa170 i64, 0x8, 0x0

(%%ssa172) ExitFunction

(%%ssa173) EndBlock %ssa3

Используемые методы

Методы	QEMU	box64	FEX
Промежуточное представление	+	-	+
Блоки трансляции	+	+	+
Связывание блоков трансляции	+	+	+
Поддержка самомодифицирующегося кода	+	+	±
Поддержка родных библиотек	-	+	+
Распространение констант	+	-	+
Устранение мертвого кода	+	-	+
Устранение загрузок контекста	-	-	+
Устранение хранения	+	-	+
Сжатие инструкций	+	-	+
Устранение временных регистров	-	-	+
Анализ живости	+	-	+

Выводы

Были рассмотрены основные методы применяемые именно в динамической трансляции. Выделены основные оптимизации и методы трансляции в открытых проектах.