Translating vm520 Branches to Intel 64

CS 520
Dept. of Computer Science
Univ. of New Hampshire

The Problem

Intel 64 instructions are variable-length

Therefore, no simple formula to derive Intel address from vm520 address.

In general, need to make one pass through vm520 code and build a table that maps vm520 address to Intel 64 address

Then go back through the translate code and fill in "holes"

ifThen.obj

VM520 addr	VM520 code	Intel 64 addr	Intel 64 code
0	00003014 jmp +3	0	E9 1B 00 00 00 00 00 00 jmp +27
1	00000000 word 0	8	00 00 00 00 00 00 00 00 .quad 0
2	00000011 word 17	16	11 00 00 00 00 00 00 00 .quad 17
3	00000021 word 33	24	21 00 00 00 00 00 00 00 .quad 33
4	FFFFD001 load r0, -3 ie addr 2	32	4C 8B 87 10 00 00 00 movq 16(%rdi), r8
5	FFFFD101 load r1, -3 ie addr 3	39	4C 8B 8F 18 00 00 00 movq 24(%rdi), r9

Vm 520

addr	code
6	00021012
	bgt r0, r1, +2
	ie addr 9
7	00 00 D2 03
	ldimm, r2, 13
8	00 00 10 14
	jmp +1
	ie addr 10
9	00 00 B2 03
	ld imm r2, 11
10	FF FF 62 02
	store r2, -10
	ie addr 1
11	00 00 00 00
	halt

Intel 64

addr	code
46	4D 39 C1
	cmpq %r8, %r9
	0F 8F [0C 00 00 00]
	4 byte "hole"
	JG [+12]
55	49 C7 C2 0D 00 00 00
	movq $13, %r10
62	E9 [07 00 00 00]
	4 byte "hole"
	JMP [+7]
67	49 C7 C2 0B 00 00 00
	movq $11, %r10
74	4C 89 97 08 00 00 00
	movq %r10, 8(%rdi)
81	C3
	ret

vm580 addr 9 → Intel addr 67

PC 55 + 12 = 67

addr 10 vm520 → addr 74 Intel

PC = 67 + 7 = 74