

The x86 language has Turing Complete memory access

An abstract machine having a tape head that can be advanced in 0 to 0x7FFFFFFF increments an unlimited number of times specifies a model of computation that has access to unlimited memory. The technical name for memory addressing based on displacement from the current memory address is relative addressing.

When we define that abstract model of computation defined by the x86 language we are only including the syntactic byte sequence for each instruction and the functional result that each instruction was defined to achieve. We are explicitly excluding the hardware implementation details of how the instruction achieves this functional end result.

Because the abstract model of computation defined by the x86 language has relative addressing for both control flow and data access this abstract model has control flow and data access to memory far outside of the boundaries of its 32-bit registers.

Jumps to an address that is 7FFFFFFF greater than FFFFFFF5

```
ffffff0: e9ffffff7f      jmp 0xffffffff5 + 0x7ffffff
ffffff5: 90              nop
```

Loads eax with data from an address 7FFFFFFF greater than FFFFFFFF

```
0000014b: bfffffff      mov ebx, 0xffffffff
00000150: 8b83ffffff7f  mov eax, dword ptr [ebx+0x7ffffff]
```

The semantics specified by the x86 language could be implemented by a memory architecture organized as an unlimited sequence of contiguous 4GB blocks. Absolute addressing modes of the 86 language would then only refer to addresses within the current 4GB block. The concept of a current 4GB block would be analogous to the current location of a Turing Machine tape head.

It is only hardware implementations of this abstract model that place any limit on memory access. These hardware limits are implementation details that are not any aspect of the abstract model itself.

The code begins @ machine address 0x100. Fills the 256 bytes preceding it with “@@@@”. Dynamically modifies its own first instruction to refer to its new code address. Copies itself to a new address that is exactly 0x100 bytes above its current code address and then does a relative jump to this new address.

The first 1024 bytes of memory are shown. Then all of the details of four complete cycles an execution trace are listed. Finally the first 1024 bytes of memory are displayed again. The x86 emulator terminates execution after these four complete cycles of execution.

According to the meaning of the syntax of the x86 language this program would continue to operate after it completed its execution @ machine address: FFFFFFF0.

The language syntax allows:

- (a) Relative Jumps as large as 0x7FFFFFFF even if the EIP = 0xFFFFFFFF0.
- (b) Data access offsets as large as 0x7FFFFFFF relative to the base register even if the Base Register = 0xFFFFFFFF.

The only reason that the code would not continue to fill unlimited memory with “@@@@” would be that the physical implementation of the abstract model specified by the x86 language did not implement the semantics specified by the x86 language syntax.

```

100:  B80010000      mov  eax, 0x100
105:  8BD8           mov  ebx, eax
107:  81EB00010000   sub  ebx, 0x100
10d:  C70340404040   mov  dword ptr [ebx], 0x40404040
113:  83C304         add  ebx, 0x4
116:  3BD8           cmp  ebx, eax
118:  7CF3           j<  0x10d
11a:  8B4801         mov  ecx, dword ptr [eax+0x1]
11d:  81C100010000   add  ecx, 0x100
123:  894801         mov  dword ptr [eax+0x1], ecx
126:  8BD8           mov  ebx, eax
128:  8BD0           mov  edx, eax
12a:  83C241         add  edx, 0x41
12d:  8B0B           mov  ecx, dword ptr [ebx]
12f:  898B00010000   mov  dword ptr [ebx+0x100], ecx
135:  83C304         add  ebx, 0x4
138:  3BDA           cmp  ebx, edx
13a:  7CF1           j<  0x12d
13c:  E9BF000000     jmp  0x200

```

1024 byte memory block prior to code execution

```

; - - memory
;
00000000: 0 1 2 3 4 5 6 7 8 9 a b c d e f
00000010: 4c 01 04 00 de 1e 44 5f 9e 03 00 00 18 00 00 00
00000020: 00 00 00 00 2e 74 65 78 74 24 6d 6e 00 00 00 00
00000030: 00 00 00 00 e2 01 00 00 b4 00 00 00 96 02 00 00
00000040: 00 00 00 00 01 00 00 00 20 00 50 60 2e 64 61 74
00000050: 61 00 00 00 00 00 00 00 00 00 00 00 29 00 00 00
00000060: a0 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000070: 40 00 50 c0 2e 64 65 62 75 67 24 53 00 00 00 00
00000080: 00 00 00 00 ac 00 00 00 c9 02 00 00 00 00 00 00
00000090: 00 00 00 00 00 00 00 00 40 00 10 42 2e 64 72 65
000000a0: 63 74 76 65 00 00 00 00 00 00 00 00 28 00 00 00
000000b0: 75 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000c0: 00 0a 00 00 55 8b ec 51 53 90 90 90 90 90 90 90
000000d0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
000000e0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
000000f0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
00000100: b8 00 01 00 00 8b d8 81 eb 00 01 00 00 c7 03 40
00000110: 40 40 40 83 c3 04 3b d8 7c f3 8b 48 01 81 c1 00
00000120: 01 00 00 89 48 01 8b d8 8b d0 83 c2 41 8b 0b 89
00000130: 8b 00 01 00 00 83 c3 04 3b da 7c f1 e9 bf 00 00
00000140: 00 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
00000150: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
00000160: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
00000170: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
00000180: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
00000190: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
000001a0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
000001b0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
000001c0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
000001d0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
000001e0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
000001f0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
00002000: f4 f4 6a 10 e8 7e 00 00 83 c4 04 89 45 fc f4
00002010: 5b 8b e5 5d c3 55 8b ec 51 8b 45 08 03 45 0c 89
00002020: 45 fc f4 8b e5 5d c3 55 8b ec 53 56 57 bb ff ff
00002030: ff ff 8b 83 ff ff ff 7f bb 38 02 00 00 8b 93 ff
00002040: ff 00 00 8b f3 8b fa 8b 06 89 07 83 c6 04 83 c7
00002050: 04 3b f3 7e f2 8b f3 c6 06 00 83 c6 04 3b f2 7c
00002060: f6 81 42 01 ff ff 00 00 ff e2 90 90 90 90 5f 5e
00002070: 5b 5d c3 55 8b ec 5d c3 55 8b ec 5d c3 55 8b ec
00002080: 5d c3 55 8b ec 5d c3 55 8b ec 5d c3 55 8b ec 5d
00002090: c3 55 8b ec 5d c3 85 01 00 00 10 00 00 00 06 00
000020a0: 11 11 11 11 22 22 22 22 2d 2d 2d 2d 45 6e 64 20
000020b0: 6f 66 20 4d 65 6d 6f 72 79 20 41 6c 6c 6f 63 61
000020c0: 74 69 6f 6e 2a 2a 2a 2a 00 04 00 00 00 f1 00 00
000020d0: 00 9d 00 00 00 62 00 01 11 00 00 00 00 44 3a 5c
000020e0: 5f 48 50 5f 53 74 72 65 61 6d 5c 5f 5f 4e 4c 55
000020f0: 5f 4e 6f 74 65 73 5c 5f 5f 57 6f 72 6b 5f 49 6e
00003000: 5f 50 72 6f 67 72 65 73 73 5c 5f 5f 48 61 6c 74
00003010: 5f 44 65 63 69 64 65 72 5f 58 38 36 5c 5f 52 65
00003020: 61 64 5f 4f 62 6a 65 63 74 5f 46 69 6c 65 5c 48
00003030: 61 6c 74 37 2e 6f 62 6a 00 37 00 3c 11 03 02 00
00003040: 00 06 00 00 00 00 00 00 00 00 00 0e 00 10 00 92
00003050: 69 01 00 4d 69 63 72 6f 73 6f 66 74 20 28 52 29
00003060: 20 4d 61 63 72 6f 20 41 73 73 65 6d 62 6c 65 72
00003070: 00 00 00 00 00 2f 44 45 46 41 55 4c 54 4c 49 42
00003080: 3a 4c 49 42 43 4d 54 20 2f 44 45 46 41 55 4c 54
00003090: 4c 49 42 3a 4f 4c 44 4e 41 4d 45 53 20 00 40 63
000030a0: 6f 6d 70 2e 69 64 92 69 03 01 ff ff 00 00 03 00
000030b0: 40 66 65 61 74 2e 30 30 10 00 00 00 ff ff 00 00
000030c0: 03 00 2e 74 65 78 74 24 6d 6e 00 00 00 00 01 00
000030d0: 00 00 03 01 e2 01 00 00 01 00 00 00 00 00 00 00
000030e0: 00 00 00 00 00 00 2e 64 61 74 61 00 00 00 00 00
000030f0: 00 00 02 00 00 00 03 01 29 00 00 00 00 00 00 00

```



```

[013a] 7cf1          j1 000012d
[012d] 8b0b          mov ecx,[ebx]
[012f] 898b00010000 mov [ebx+00000100],ecx
[0135] 83c304        add ebx,+04
[0138] 3bda          cmp ebx,edx
[013a] 7cf1          j1 000012d
[012d] 8b0b          mov ecx,[ebx]
[012f] 898b00010000 mov [ebx+00000100],ecx
[0135] 83c304        add ebx,+04
[0138] 3bda          cmp ebx,edx
[013a] 7cf1          j1 000012d
[012d] 8b0b          mov ecx,[ebx]
[012f] 898b00010000 mov [ebx+00000100],ecx
[0135] 83c304        add ebx,+04
[0138] 3bda          cmp ebx,edx
[013a] 7cf1          j1 000012d
[012d] 8b0b          mov ecx,[ebx]
[012f] 898b00010000 mov [ebx+00000100],ecx
[0135] 83c304        add ebx,+04
[0138] 3bda          cmp ebx,edx
[013a] 7cf1          j1 000012d
[012d] 8b0b          mov ecx,[ebx]
[012f] 898b00010000 mov [ebx+00000100],ecx
[0135] 83c304        add ebx,+04
[0138] 3bda          cmp ebx,edx
[013a] 7cf1          j1 000012d
[012d] 8b0b          mov ecx,[ebx]
[012f] 898b00010000 mov [ebx+00000100],ecx
[0135] 83c304        add ebx,+04
[0138] 3bda          cmp ebx,edx
[013a] 7cf1          j1 000012d
[012d] 8b0b          mov ecx,[ebx]
[012f] 898b00010000 mov [ebx+00000100],ecx
[0135] 83c304        add ebx,+04
[0138] 3bda          cmp ebx,edx
[013a] 7cf1          j1 000012d
[012d] 8b0b          mov ecx,[ebx]
[012f] 898b00010000 mov [ebx+00000100],ecx
[0135] 83c304        add ebx,+04
[0138] 3bda          cmp ebx,edx
[013a] 7cf1          j1 000012d
[012d] 8b0b          mov ecx,[ebx]
[012f] 898b00010000 mov [ebx+00000100],ecx
[0135] 83c304        add ebx,+04
[0138] 3bda          cmp ebx,edx
[013a] 7cf1          j1 000012d
[012d] 8b0b          mov ecx,[ebx]
[012f] 898b00010000 mov [ebx+00000100],ecx
[0135] 83c304        add ebx,+04
[0138] 3bda          cmp ebx,edx
[013a] 7cf1          j1 000012d
[012d] 8b0b          mov ecx,[ebx]
[012f] 898b00010000 mov [ebx+00000100],ecx
[0135] 83c304        add ebx,+04
[0138] 3bda          cmp ebx,edx
[013a] 7cf1          j1 000012d
[012d] 8b0b          mov ecx,[ebx]
[012f] 898b00010000 mov [ebx+00000100],ecx
[0135] 83c304        add ebx,+04
[0138] 3bda          cmp ebx,edx
[013a] 7cf1          j1 000012d
[013c] e9bf000000    jmp 00000200
[0200] b800020000    mov eax,00000200
[0205] 8bd8          mov ebx,eax
[0207] 81eb00010000 sub ebx,00000100
[020d] c70340404040 mov [ebx],40404040
[0213] 83c304        add ebx,+04

```



```

[0216] 3bd8          cmp ebx,eax
[0218] 7cf3          j1 000020d
[020d] c703404040   mov [ebx],40404040
[0213] 83c304       add ebx,+04
[0216] 3bd8          cmp ebx,eax
[0218] 7cf3          j1 000020d
[020d] c703404040   mov [ebx],40404040
[0213] 83c304       add ebx,+04
[0216] 3bd8          cmp ebx,eax
[0218] 7cf3          j1 000020d
[020d] c703404040   mov [ebx],40404040
[0213] 83c304       add ebx,+04
[0216] 3bd8          cmp ebx,eax
[0218] 7cf3          j1 000020d
[020d] c703404040   mov [ebx],40404040
[0213] 83c304       add ebx,+04
[0216] 3bd8          cmp ebx,eax
[0218] 7cf3          j1 000020d
[020d] c703404040   mov [ebx],40404040
[0213] 83c304       add ebx,+04
[0216] 3bd8          cmp ebx,eax
[0218] 7cf3          j1 000020d
[020d] c703404040   mov [ebx],40404040
[0213] 83c304       add ebx,+04
[0216] 3bd8          cmp ebx,eax
[0218] 7cf3          j1 000020d
[020d] c703404040   mov [ebx],40404040
[0213] 83c304       add ebx,+04
[0216] 3bd8          cmp ebx,eax
[0218] 7cf3          j1 000020d
[021a] 8b4801       mov ecx,[eax+01]
[021d] 81c100010000 add ecx,00000100
[0223] 894801       mov [eax+01],ecx
[0226] 8bd8          mov ebx,eax
[0228] 8bd0          mov edx,eax
[022a] 83c241       add edx,+41
[022d] 8b0b          mov ecx,[ebx]
[022f] 898b00010000 mov [ebx+00000100],ecx
[0235] 83c304       add ebx,+04
[0238] 3bda          cmp ebx,edx
[023a] 7cf1          j1 000022d
[022d] 8b0b          mov ecx,[ebx]
[022f] 898b00010000 mov [ebx+00000100],ecx
[0235] 83c304       add ebx,+04
[0238] 3bda          cmp ebx,edx
[023a] 7cf1          j1 000022d
[022d] 8b0b          mov ecx,[ebx]
[022f] 898b00010000 mov [ebx+00000100],ecx
[0235] 83c304       add ebx,+04
[0238] 3bda          cmp ebx,edx
[023a] 7cf1          j1 000022d
[022d] 8b0b          mov ecx,[ebx]
[022f] 898b00010000 mov [ebx+00000100],ecx
[0235] 83c304       add ebx,+04
[0238] 3bda          cmp ebx,edx
[023a] 7cf1          j1 000022d
[022d] 8b0b          mov ecx,[ebx]
[022f] 898b00010000 mov [ebx+00000100],ecx
[0235] 83c304       add ebx,+04

```


