The MIPS R4000, part 10: Trampolines and stubs

devblogs.microsoft.com/oldnewthing/20180413-00

April 13, 2018

Raymond Chen

We saw earlier that the relative branch instructions have a reach of ±128KB, but what if the function you want to call is further away than that?

The linker detects that the branch target is too far away and creates a trampoline stub, the same way the Alpha AXP compiler did. The branch instruction is then rewritten to be a branch to the trampoline, and the trampoline performs another jump to the final destination.

```
    BAL     dest_trampoline ; was "BAL dest"
...
dest_trampoline:
    J       dest
    NOP                     ; branch delay slot
```

The limited reach of the relative branch instructions means that a single function cannot be larger than 256KB.

On the other hand, the existence of the `JAL` instruction means that the compiler doesn't really need to use `BAL` at all. Trampolines come into play only with conditional calls, and those are relatively rare.

If a function is naïvely-imported, then the compiler will generate a normal branch-and-link instruction, and the import library will provide a stub that in turn jumps indirectly through the import table. Doing this requires a scratch register, and that's where the *at* register once again enters the picture:

```
    BAL     imported_function_stub
...

imported_function_stub:
    LUI     at, XXXX
    LW      at, YYYY(at)    ; load from import address table
    JR      at              ; and jump there
    NOP                     ; branch delay slot
```

Where `XXXX` and `YYYY` are computed in the usual way, namely, so that `(XXXX << 16) + (int16_t)YYYY` is the address of the import address table entry.

If you are unlucky enough that you are calling an imported function naïvely, *and* the imported stub is beyond the reach of the `BAL` instruction, then you will have to bounce through two trampolines! The first was generated by the linker to help you reach the stub, and the second came from the import library to get you from the stub to the final destination.

This double-trampoline could also happen on the Alpha AXP, but it was less common because the Alpha AXP's relative branch instructions have a reach of ±4MB, as opposed to the MIPS R4000's relative branch instructions, which can reach only ±128KB.

Raymond Chen

Follow