

Chapter 1

Code generation

1.1 Stack machines

A stack machine uses only a stack as storage. When executing an instruction $r = F(a_1, \dots, a_n)$, it pops n operands from the stack, computes the operation F using the operands, and pushes the result r back on the stack. For example, when computing $7 + 5$, the stack will change from $s-7-5$ to $s-12$.

Consider two instructions: `push i` (push integer i on the stack) and `add` (add two integers). Then we have the program to compute $7 + 5$:

```
push 7
push 5
add
```

An important property of stack machines is that location of the operands/result is not explicitly stated because they are always at the top of the stack. This is different from register machine in which the locations have to be specified. We have `add` instead of `add r1, r2, r3`, which produces more compact programs. This is one of the reasons why JAVA bytecodes uses stack evaluation.

Stack machine produces compact programs, but register machine executes faster. There is an intermediate point between the two kinds of machines called an **n-register stack machine**. As the name reveals, the top n positions of the pure stack machine's stack are held in registers. It turns out that even one single register can provide considerable performance improvement, which is the case of **1-register stack machine**. The register is called the **accumulator**.

In a pure stack machine, an `add` does 3 memory operations: two reads and one write. But in a 1-register stack machine, what `add` does is `acc ← acc + top_of_stack`. In general, consider an arbitrary expression `op(e1, ..., en)`. For each subexpression e_i ($1 \leq i \leq n-1$), we will compute e_i , store the result in `acc` and then push the result on the stack. For e_n , we will have its result remain in `acc`. Then we will pop $n-1$ values from the stack to compute `op`, and store the result in `acc`. If we follow this procedure, obviously after evaluating an

expression e , acc holds the value of e , and the stack is unchanged. In other words, **expression evaluation preserves the stack**.

Consider the calculation of $3 + (7 + 5)$. We will have the following process:

Code	Acc	Stack
$acc \leftarrow 3$	3	<init>
push acc	3	3,<init>
$acc \leftarrow 7$	7	3,<init>
push acc	7	7,3,<init>
$acc \leftarrow 5$	5	7,3,<init>
$acc \leftarrow acc + top_of_stack$	12	7,3,<init>
pop	12	3,<init>
$acc \leftarrow acc + top_of_stack$	15	3,<init>
pop	15	<init>

1.2 Basic MIPS instructions

In our discussion of code generation, we will focus on generating code for a stack machine with accumulator. The resulting code should be able to run on an MIPS processor (or simulator). Thus we have to simulate stack machine instructions using MIPS instructions and registers.

We choose to keep the accumulator in MIPS register $\$a0$. The stack is kept in memory and grows towards lower addresses, which is a standard convention in MIPS. The address of the next location on the stack is kept in MIPS register $\$sp$ (which stands for stack pointer), and the top of the stack is at address $\$sp + 4$.

MIPS is an old structure with a relatively simple instruction set (prototypical reduced instruction set computer, or RISC). Most MIPS operations use registers for operands and results. Load and store instructions are used to move values to and from memory. There are 32 general purpose registers (32 bits each) in MIPS, and we will use only $\$a0$, $\$sp$ and $\$t1$ (temp register used for operations that take two arguments).

Here are the first set of MIPS instructions that we introduce.

lw $reg1$ offset($reg2$) : Load 32-bit word from address $reg2 + offset$ into $reg1$.

sw $reg1$ offset($reg2$) : Store 32-bit word in $reg1$ at address $reg2 + offset$.

add $reg1$ $reg2$ $reg3$: $reg1 \leftarrow reg2 + reg3$

addiu $reg1$ $reg2$ imm : $reg1 \leftarrow reg2 + imm$. u means that overflow is not checked.

li reg imm : $reg \leftarrow imm$.

move $reg1$ $reg2$ $reg1 \leftarrow reg2$.

The stack machine code for $7 + 5$ is:

$\text{acc} \leftarrow 7$	<code>li \$a0 7</code>
<code>push acc</code>	<code>sw \$a0 0(\$sp)</code>
	<code>addiu \$sp \$sp -4</code>
$\text{acc} \leftarrow 5$	<code>li \$a0 5</code>
$\text{acc} \leftarrow \text{acc} + \text{top_of_stack}$	<code>lw \$t1 4(\$sp)</code>
	<code>add \$a0 \$a0 \$t1</code>
<code>pop</code>	<code>addiu \$sp \$sp 4</code>

1.3 Code generation

In this section we will take a look at code generation for higher level languages rather than a simple stack machine in the previous section.

Consider a language for integer operations. Its grammar depicts a list of function definitions:

$$\begin{aligned}
 P &\rightarrow D; P \mid D \\
 D &\rightarrow \text{def id}(\text{ARGS}) = E; \\
 \text{ARGS} &\rightarrow \text{id}, \text{ARGS} \mid \text{id} \\
 E &\rightarrow \text{int} \mid \text{id} \mid \text{if } E_1 = E_2 \text{ then } E_3 \text{ else } E_4 \mid E_1 + E_2 \mid E_1 - E_2 \mid \text{id}(E_1, \dots, E_n)
 \end{aligned}$$

The first function definition f is the entry point, i.e. the `main` routine. This language is enough to write a program that computes the Fibonacci numbers:

$$\begin{aligned}
 \text{def fib}(x) = & \text{if } x = 1 \text{ then } 0 \text{ else} \\
 & \text{if } x = 2 \text{ then } 1 \text{ else} \\
 & \text{fib}(x - 1) + \text{fib}(x - 2)
 \end{aligned}$$

For each expression e , we want to generate MIPS code that **computes the value of e in $\$a0$ and preserves $\$sp$ and the content of the stack**. We will define a function $\text{cgen}(e)$ whose return value is the code generated for e .

1.3.1 Constants

For constants, we need to simply load it into the accumulator:

$$\text{cgen}(i) = \text{li } \$a0 \ i$$

1.3.2 Addition

For addition:

```
cgen(e1 + e2) =  
cgen(e1)  
sw $a0 0($sp)  
addiu $sp $sp -4  
cgen(e2)  
lw $t1 4($sp)  
add $a0 $t1 $a0  
addiu $sp $sp 4
```

Here we use different colors to emphasize the fact that MIPS code is **generated** at compile time and **executed** at run time. Code in red color is what happens at compile time: the generation, while code in black is what happens at run time: the execution. More precisely, we should write `sw $a0 0($sp)` as something like `print sw $a0 0($sp)`, which indicates that the MIPS code is generated at compile time and saved somewhere, maybe in an intermediate file, and does not get executed until run time.

It seems that the piece of code above could be optimized: why don't we save the value of `e1` directly in `$t1`, rather than saving it in the memory and then retrieve it into `$t1`? The code will look like:

```
cgen(e1 + e2) =  
cgen(e1)  
move $t1 $a0  
cgen(e2)  
add $a0 $t1 $a0
```

Unfortunately, this neat piece of code is wrong. We can convince ourselves by simply considering the code generated for `1 + (2 + 3)`. In short, the value of `$t1` will be modified during `cgen(e2)`, and is no longer the value of `e1` when the execution comes to `add $a0 $t1 $a0`.

The simple example of code generation for addition demonstrates a few universal properties of code generation. The code generated for `e1 + e2` is a template with “holes” for code generated to evaluate `e1` and `e2`. Stack machine code generation is actually recursive. The code generation process can be written as a recursive descent of the AST, at least for expressions.

1.3.3 Subtraction

By introducing another MIPS instruction `sub`:

```
sub reg1 reg2 reg3 reg1 ← reg2 - reg3
```

we can generate the code for $e1 - e2$:

```
cgen(e1 - e2) =  
    cgen(e1)  
    sw $a0 0($sp)  
    addiu $sp $sp -4  
    cgen(e2)  
    lw $t1 4($sp)  
    sub $a0 $t1 $a0  
    addiu $sp $sp 4
```

1.3.4 If-then-else

In order to generate code for if-then-else expressions, we need to introduce a couple of new instructions:

beq reg1 reg2 label branch to label if $reg1 = reg2$

b label Unconditional jump to label

```
cgen(if e1 = e2 then e3 else e4) =  
    cgen(e1)  
    sw $a0 0($sp)  
    addiu $sp $sp -4  
    cgen(e2)  
    lw $t1 4($sp)  
    addiu $sp $sp 4  
    beq $t1 $a0 true_branch  
false_branch:  
    cgen(e4)  
    b end_if  
true_branch:  
    cgen(e3)  
end_if:
```

1.3.5 Function calls & definitions, variable references

Code for function calls and function definitions depends on the layout of the activation record, thus they need to be designed together. For this simple language, a very simple AR is sufficient.

- Since the result is always in the accumulator, there is no need to store the result in AR.

- The AR should hold the actual parameters, thus for $f(x_1, \dots, x_n)$, we need to push x_n, \dots, x_1 on the stack. These are the only variables in this language.
- The stack discipline guarantees that `$sp` is preserved after a function call. Thus there is no need for a control link: the previous activation can be found directly; and we do not need to look at another activation during the function call because there is no local variable.
- We need the return address.
- A pointer to the current activation is useful. It lives in register `$fp` (frame pointer).

To summarize, an AR will contain the caller's frame pointer, the actual parameters and the return address. Consider a call to $f(x, y)$. The AR is

```

cgen(f(e1,e2,...,en)) =
    sw $fp 0($sp)
    addiu $sp $sp -4
    cgen(en)
    sw $a0 0($sp)
    addiu $sp $sp -4
    ...
    cgen(e1)
    sw $a0 0($sp)
    addiu $sp $sp -4
    jal f_entry

```

```

cgen(def f(x1,x2,...,xn) = e) =
f_entry:
    move $fp $sp
    sw $ra 0($sp)
    addiu $sp $sp -4
    cgen(e)
    lw $ra 4($sp)
    addiu $sp $sp 4n + 8
    lw $fp 0($sp)
    jr $ra
cgen(xi) = lw $a0 4*i($fp)

```