CSE443
Compilers

Dr. Carl Alphonce
alphonce@buffalo.edu
343 Davis Hall
Phases of a compiler

Intermediate Representation (IR): specification and generation

Figure 1.6, page 5 of text
# Stack frame organization

<table>
<thead>
<tr>
<th>Stack Frame Organization</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>actual parameters</td>
<td>(arguments)</td>
</tr>
<tr>
<td>returned value</td>
<td></td>
</tr>
<tr>
<td>control link</td>
<td>(dynamic link)</td>
</tr>
<tr>
<td>access link</td>
<td>(static link)</td>
</tr>
<tr>
<td>saved machine status</td>
<td>(return address)</td>
</tr>
<tr>
<td>local data</td>
<td></td>
</tr>
<tr>
<td>temporaries</td>
<td></td>
</tr>
</tbody>
</table>

- **Initialized by caller, used by callee.**
- **May be in CPU registers.**
## Stack frame organization

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>actual parameters</strong></td>
<td>Arguments</td>
</tr>
<tr>
<td><strong>returned value</strong></td>
<td>Initialized by callee, read by caller.</td>
</tr>
<tr>
<td><strong>control link</strong></td>
<td>(Dynamic link)</td>
</tr>
<tr>
<td><strong>access link</strong></td>
<td>(Static link)</td>
</tr>
<tr>
<td><strong>saved machine status</strong></td>
<td>(Return address)</td>
</tr>
<tr>
<td><strong>local data</strong></td>
<td></td>
</tr>
<tr>
<td><strong>temporaries</strong></td>
<td></td>
</tr>
</tbody>
</table>

- **Initialized by callee, read by caller.**
- **May be in a CPU register.**
**Stack frame organization**

<table>
<thead>
<tr>
<th><strong>actual parameters</strong></th>
<th><strong>returned value</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>(arguments)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>control link</strong></th>
<th><strong>access link</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>(dynamic link)</td>
<td>(static link)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>saved machine status</strong></th>
<th><strong>local data</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>(return address)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>temporaries</strong></th>
</tr>
</thead>
</table>

The address of the caller's invocation record (stack frame).
Stack frame organization

- actual parameters (arguments)
- returned value
- control link (dynamic link)
- access link (static link)
- saved machine status (return address)
- local data
- temporaries

Used to achieve static scope for nested function definitions.
Our language does not use this.
Scheme/ML do.
## Stack frame organization

<table>
<thead>
<tr>
<th></th>
<th>Information needed to restore machine to state at function call, including the return address (the value of the Program Counter at the time of the call).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>actual parameters</strong> (arguments)</td>
<td></td>
</tr>
<tr>
<td><strong>returned value</strong></td>
<td></td>
</tr>
<tr>
<td><strong>control link</strong> (dynamic link)</td>
<td></td>
</tr>
<tr>
<td><strong>access link</strong> (static link)</td>
<td></td>
</tr>
<tr>
<td><strong>saved machine status</strong> (return address)</td>
<td></td>
</tr>
<tr>
<td><strong>local data</strong></td>
<td></td>
</tr>
<tr>
<td><strong>temporaries</strong></td>
<td></td>
</tr>
</tbody>
</table>
Stack frame organization

- actual parameters (arguments)
- returned value
- control link (dynamic link)
- access link (static link)
- saved machine status (return address)
- local data
- temporaries

Space for local variables.
## Stack frame organization

<table>
<thead>
<tr>
<th>Stack Frame Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>actual parameters (\text{(arguments)})</td>
</tr>
<tr>
<td>returned value</td>
</tr>
<tr>
<td>control link (\text{(dynamic link)})</td>
</tr>
<tr>
<td>access link (\text{(static link)})</td>
</tr>
<tr>
<td>saved machine status (\text{(return address)})</td>
</tr>
<tr>
<td>local data</td>
</tr>
<tr>
<td>temporaries</td>
</tr>
</tbody>
</table>

- **Space for temporary variables, and variable-length local data**
- **Temporaries may be in CPU registers.**
7.2.3 Calling Sequence

What happens during a function call?
caller's invocation record

Prior to function call.
7.2.3 Calling Sequence

"Procedure calls are implemented by what are known as calling sequences, which consist of code that allocates an activation record on the stack and enters information into its fields."

[p. 436]
During function call.
7.2.3 Calling Sequence

"A return sequence is similar code to restore the state of the machine so the calling procedure can continue its execution after the call."

[p. 436]
caller's invocation record

top_sp

top

After function call.
"In general, if a procedure is called from n different points, then the portion of the calling sequence assigned to the caller is generated n times. However, the portion assigned to the callee is generated only once."
Typical calling sequence [p. 437]

"1. The caller evaluates the actual parameters."

Recall:

formal parameter == parameter

actual parameter == argument
Prior to function call.
Caller writes arguments (actual parameters) past the end of its own invocation record.
Typical calling sequence [p. 437]

"2. The caller stores a return address and the old value of top_sp into the callee's activation record. The caller then increments top_sp […] top_sp is moved past the caller's local data and temporaries and the callee's parameters and status fields."
Caller knows the offset of the eventual returned value. When callee returns the caller will look at this location for the returned value.
"2. The caller stores a return address and the old value of top_sp into the callee's activation record. ... "
The caller stores its stack pointer here.
The caller stores its stack pointer here. When the callee finishes the stack pointer's value will be reset to this value, thereby restoring the caller's invocation record as the active one (the one on top of the stack).
2. The caller stores a return address and the old value of top_sp into the callee's activation record. The caller then increments top_sp [...] top_sp is moved past the caller's local data and temporaries and the callee's parameters and status fields.
caller's invocation record

- actual parameters
- returned value
- control link
- access link
- saved machine status
- local data
- temporaries

Move top_sp

- top_sp
- top

- caller's invocation record

© 2022 Carl Alphonce - Reproduction of this material is prohibited without the author's consent
Typical calling sequence [p. 437]

"3. The callee saves the register values and other status information."
Write the return address, the current value of the Program Counter (PC), into the saved machine status. When the callee finishes execution will resume with the address pointed to by this saved address.
When control transfers to the callee, the top_sp and top are updated.

Callee writes local data and temporaries into its invocation record.
If the number of arguments can vary from call to call (e.g. printf) then the caller writes the arguments to the "actual parameters" area, as well as information about the number of arguments to the status area.
If the callee has variable length local data (e.g. local arrays whose size is determined by the value of a parameter) then the arrays are allocated space at the end of the invocation record, and pointers to those arrays are stored in the "locals" block.
Relocatable object code

- Compiler produces relocatable object code: addresses are not absolute, but relative to known boundaries (e.g. Stack Pointer, start of record, Program Counter).

- Linker combines object code files into an executable file, in which static relative addresses are made absolute (in virtual address space).

- Loader copies contents of executable file into memory and starts execution.
Relocatable object code

- Compiler produces **relocatable object code**: addresses are not absolute, but relative to known boundaries (e.g. Stack Pointer, start of record, Program Counter).

- Linker combines object code files into executable file, in which static relative addresses are made absolute (in virtual address space).

- Loader copies contents of executable file into memory and starts execution.

   Leave relative offsets alone during translation.
Target Architecture

Code Generation

- We will generate x86-64 assembly
- Examples will not always show x86-64 assembly
Desirable characteristics of generated code:

- correctness (this is non-negotiable)
- small execution time
- small code size
- small power consumption
Desirable characteristics of generated code:

- Correctness (this is non-negotiable)
- Small execution time
- Small code size
- Small power consumption

Associate costs with each instruction, then "minimize" (lower) overall cost, with some balance since execution time and code size can be in conflict.
Significant tasks of code generator

- instruction selection
- register allocation and assignment
- instruction ordering
Significant tasks of code generator

Which variables are kept in registers?

- instruction selection
- register allocation and assignment
- instruction ordering
Significant tasks of code generator:

- Instruction selection
- Register allocation and assignment
- Instruction ordering

Which specific register holds which value?
Significant tasks of code generator

- instruction selection
- register allocation and assignment
- instruction ordering

E.g. to minimize the number of registers needed.
Simple generation strategy vs. code size

If we generate code for each intermediate code instruction in isolation and string the results together the result may include redundant instructions
Consider:

\[ x = y + z \]

This might be translated as:

- **LD R0, y**
  - load the value of y into register R0
- **ADD R0, R0, z**
  - put into R0 the result of adding R0 and the value of z
- **ST x, R0**
  - store the value of register R0 to x
Consider applying the same template to a larger example:

\[ a = b + c \]
\[ d = a + e \]

This might be translated as:

```
LD R0, b
ADD R0, R0, c
ST a, R0
LD R0, a
ADD R0, R0, e
ST d, R0
```
Consider applying the same template to a larger example:

\[
\begin{align*}
    a &= b + c \\
    d &= a + e \\
\end{align*}
\]

This might be translated as:

\[
\begin{align*}
    \text{LD } R0, b \\
    \text{ADD } R0, R0, c \\
    \text{ST } a, R0 \\
    \text{LD } R0, a \\
    \text{ADD } R0, R0, e \\
    \text{ST } d, R0 \\
\end{align*}
\]

This instruction is redundant: it is loading into R0 the value that is already there.