Linguagens de montagem
Procedimentos e funções

Ricardo Anido
Instituto de Computação
Unicamp

Procedimentos e funções

Uma chamada de procedimento envolve dois trechos de programas, o trecho de programa que executa a chamada e o procedimento que é chamado.

- o trecho de programa que executa a chamada
- o procedimento que é chamado.

```
int x,y,z; // declaração de algumas variáveis

void troca(int *a, int *b) {
    int tmp;

    tmp = *a;
    *a = *b;
    *b = tmp;
}

int main(void) {
    ...
    troca(&x,&y);
    z=x+1;
    troca(&z,&x);
    x=y-1;
    ...
}
```

Procedimentos e funções

A invocação de um procedimento envolve dois desvios no fluxo de execução de um programa

- na chamada do procedimento há um desvio para o início do procedimento,
- ao final da execução do procedimento o fluxo é desviado de volta para o comando seguinte à chamada de procedimento.
- o endereço para o qual o fluxo de execução deve ser desviado ao final do procedimento é chamado de *endereço de retorno* do procedimento.

Procedimentos

- O comando em linguagem de montagem para a instrução de chamada de procedimento é BL (do inglês *branch and link*).
- Essa instrução é similar a uma instrução de desvio, mas antes de executar o desvio a instrução copia o registrador `pc` para o registrador `r14`, também chamado de *link register*, `lr`.
- O formato geral do comando em linguagem de montagem é igual ao comando de desvio com endereço alvo constante:

$$BL\{cond\} \quad endereço$$

Chamada de procedimento

- Ao final da execução do procedimento, para retornar da chamada, podemos recuperar o endereço de retorno, armazenado no registrador `lr` e desviar para esse endereço usando uma instrução de desvio indireto por registrador, usando o registrador `lr`.

Chamada de procedimento

```
    bl  proc          @ uma chamada ao procedimento
                      @ de nome proc
    and r1,r2         @ esta é a instrução que deve
                      @ ser executada logo após retorno
                      @ do procedimento
    ...

     .org 0x4000
@ aqui é o início do procedimento
proc:
     mov   r5,#-1     @ esta é a primeira instrução
                      @ do procedimento
    ...
                      @ aqui é o final do procedimento
                      @ efetua retorno para endereço armazenado
     bx   lr          @ desvia para o endereço armazenado, retornando do proc
```

Procedimentos

Exemplos:

```
   blpl calcula              @ chamada de procedimento condicional
   bl   imprime              @ chamada de procedimento incondicional
   ...
calcula:                     @ um procedimento
   ...
imprime:                     @ outro procedimento
   ...
```

Problemas?

Um grande problema: não permite recursão!
Como permitir recursão?

Pilhas

Podemos implementar uma pilha usando um apontador, como `r0`. Inicialmente, ele deve ser inicializado para apontar para uma região de memória disponível.

- Uma palavra é empilhada na pilha apontada por `r0` decrementando-se `r0` de quatro e escrevendo-se a palavra no novo endereço apontado por `r0`.
- Neste esquema, a pilha "cresce" de endereços altos para endereços baixos.

Pilhas

Operação *Empilhar*:

```
@ implementando uma pilha com o registrador r0 como apontador de pilha
@ exemplo que coloca na pilha o valor corrente do registrador r10
     sub   r0,#4            @ faz apontador de pilha apontar para
                            @ novo elemento
     str   r10,[r0]         @ e coloca valor de r10 no topo da pilha


@ ou, usando pré-indexação:
     ldr    r10,[r0,#-4]!   @ armazena r10 no topo da pilha
```

Pilhas

Operação *Desempilhar*:

```
@ implementando uma pilha com o registrador r0 como apontador de pilha
@ exemplo que retira o valor do topo da pilha e armazena em r9
     ldr    r9,[r0]         @ carrega r9 com valor no topo da pilha
     add    r0,#4           @ r0 aponta para novo topo da pilha


@ ou, usando pós-indexação:
     ldr    r9,[r0],#4      @ carrega r9 com valor no topo da pilha
```

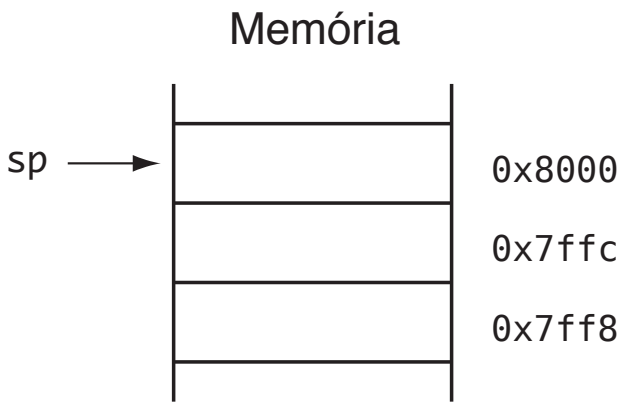
Pilhas

- manipulações de pilhas são tão frequentes que os processadores incluem instruções específicas e um registrador especial, normalmente chamado `sp` (do inglês *stack pointer*), que funciona como apontador de pilha.
- no ARM o apontador de pilha é na verdade um dos registradores de uso geral, `r13`.
- a linguagem de montagem aceita `sp` como outro nome do registrador `r13`.
- duas instruções no ARM (há muitas outras!): PUSH (empilha registradores) e POP (desempilha registradores).

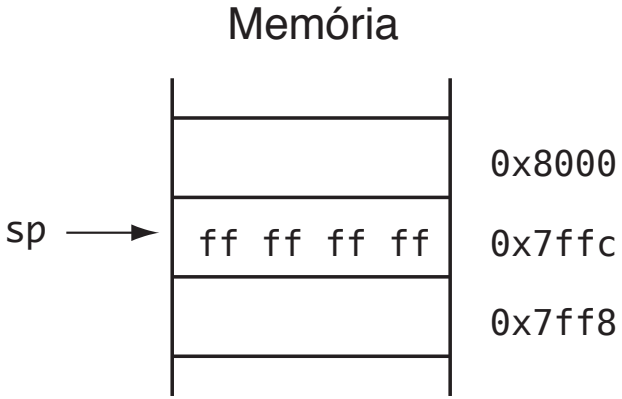
Pilhas

```
1  @ exemplos de instruções push e pop
2      mov  sp, #0x80000 @ um valor inicial para sp (final da m
3                        @ e vamos colocar um valor
4      mov  r2, #-1      @ em r2 para ilustrar
5      push r2
6      pop  r1           @ qual o valor de r1?
```

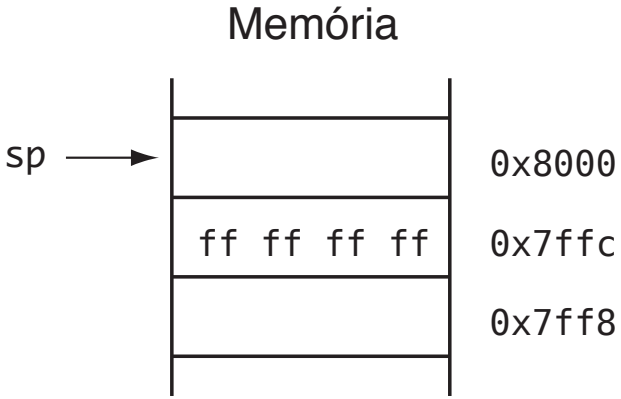
Pilhas



(a) Após a linha 2



(b) Após a linha 5



(c) Após a linha 6

Pilhas

Antes de utilizar instruções que manipulam a pilha, é necessário reservar a região de memória que será utilizada pela pilha, e inicializar o valor do registrador sp, como por exemplo:

```
@ aloca uma região da memória para a pilha
@ assume que a pilha utilizará no máximo 1 KiB
        .equ TAM_PILHA,1024
@ aloca espaço (em área de memória reservada para dados)
fim_pilha:
        .skip  TAM_PILHA
ini_pilha:
        ...
@ inicializa apontador de pilha, antes de executar
@ qualquer instrução que manipule a pilha
        ldr  sp,=ini_pilha
```

Problema

Escreva um procedimento `zera_regs` para zerar os registradores `r0`, `r1`, `r2` e `r3`.

Solução

```
@ ********
@ zera_regs
@ ********
@ Zera os registradores r0, r1, r2 e r3
@   entrada: nenhuma
@   saída: r0, r1, r2 e r3 zerados
@   destrói: nada

zera_regs:
      mov r0,#0
      mov r1,#0
      mov r2,#0
      mov r3,#0
      bx  lr
...
@ exemplo de chamada do procedimento zera_regs
      bl   zera_regs          @ após a chamada, r0=r1=r2=r3=0
```

Procedimentos com parâmetros

- Uma primeira abordagem é usar registradores para armazenar os argumentos na chamada do procedimento.
- Bastante eficiente, e pode ser usado se o procedimento não é recursivo e há registradores disponíveis em número suficiente para acomodar os parâmetros.

Problema

Escreva um procedimento `preenche_mem`, com funcionalidade similar ao procedimento *memset*, da biblioteca padrão de C. Ou seja, o procedimento `preenche_mem` deve preencher uma região de memória com um valor de byte passado como parâmetro. Os parâmetros são passados por registradores; `r0` contém o valor do byte a ser usado no preenchimento, `r1` contém endereço inicial da região de memória, `r2` contém o número de bytes a serem preenchidos com o valor dado.

Solução

```
@ ************
@ preenche_mem
@ ************
preenche_mem:
     strb   r0,[r1],#1          @ preenche um byte com valor dado
                                @ e avança apontador para próximo caractere
     subs   r2,#1               @ continua a preencher?
     bne    preenche_mem        @ desvia se ainda não terminou de preencher
     bx     lr                  @ e retorna, região foi preenchida
```

Solução

```
...                     @ prepara registradores com valores dos argumen
mov  r0,#0xff           @ valor a ser usado no preenchimento
mov  r1,#0x1000         @ endereço inicial do trecho a ser preenchido
mov  r2,#3              @ número de bytes a preencher
bl   preenche_mem       @ e chama o procedimento
...
```

Passagem de parâmetros

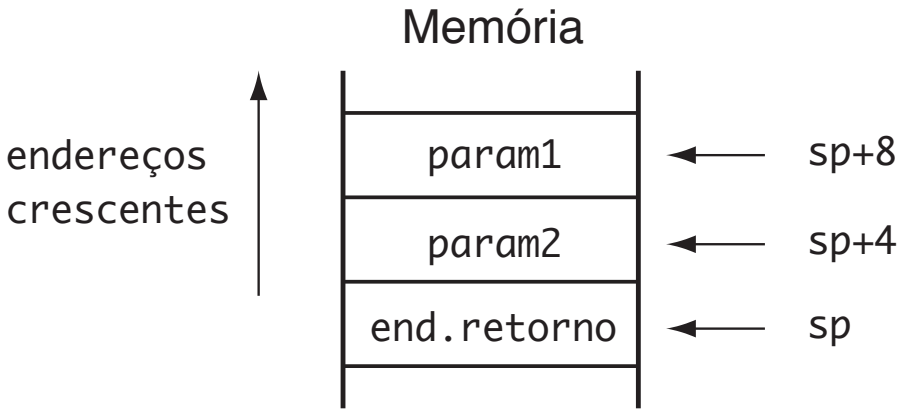
- Apesar de eficiente, a passagem de parâmetros por registradores não pode ser utilizada em todos os casos:
  - procedimentos recursivos
  - número de argumentos é maior do que o número de registradores disponíveis
- Nesses casos, é necessário utilizar a pilha para passagem de parâmetros.

Passagem de parâmetros pela pilha

- Para passar parâmetros utilizando a pilha, devemos empilhar os parâmetros antes da chamada do procedimento.
- Dentro do procedimento, podemos acessar os parâmetros utilizando o registrador apontador de pilha.
- Se procedimento não é "folha", o endereço de retorno da chamada (presente no registrador `lr`) também deve ser armazenado na pilha, pois o registrador `lr` será sobrescrito na próxima chamada a procedimento.

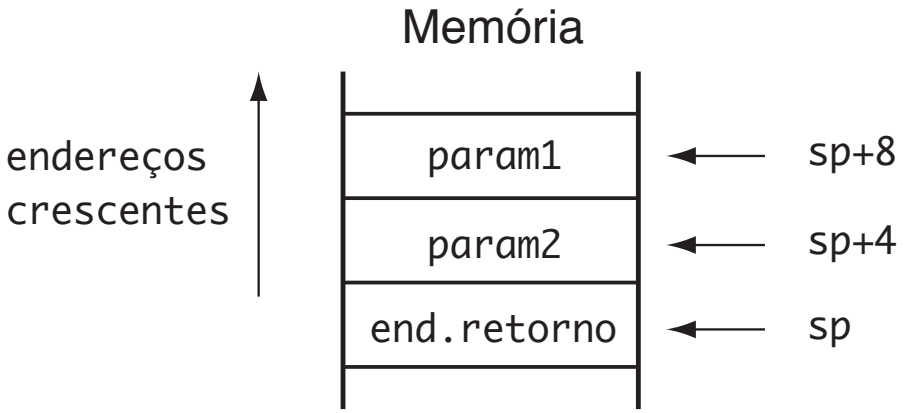
Passagem de parâmetros pela pilha

```
@ supondo que param1 esteja armazenado em r4 e param2 armazenado em r5
@ exemplo de chamada de procedimento
      push r4          @ empilha arg1 correspondente ao param1
      push r5          @ empilha arg2 correspondente ao param2
      bl   proc_param  @ agora efetua a chamada
      ...
```



Passagem de parâmetros pela pilha

```
@ Acesso a parâmetros durante a execução do procedimento.
        ...
proc_param:
        push lr             @ armazena o endereço de retorno na pilha
        ldr  r0,[sp,#8]     @ carrega valor de param2 em r0
        ldr  r1,[sp,#4]     @ e carrega valor de param1 em r1
        ...
        pop  lr             @ no retorno, recupera endereço de retorno
        bx   lr             @ e retorna
```

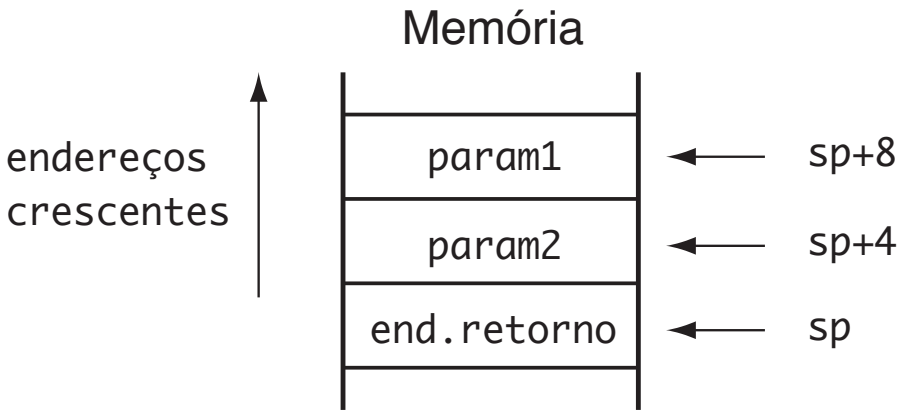


Passagem de parâmetros pela pilha

- A instrução POP NÃO deve ser usada para acessar os parâmetros na pilha, pois o endereço de retorno possívelmente está na pilha (poderá ser empilhado após os parâmetros, no início do procedimento, se o procedimento não é "folha")
- Os parâmetros empilhados antes da chamada devem permanecer na pilha até o retorno do procedimento, quando devem então ser desempilhados.

Passagem de parâmetros pela pilha

```
@ supondo que o argumento correspondente a param1 esteja armazenado em r4
@ e o argumento correspondente a param2 esteja armazenado em r5
@ exemplo de chamada de procedimento
      push r4,r5      @ empilha valor para param1 e param2
      bl   proc_param @ agora efetua a chamada
      add  sp,#8      @ retira os parâmetros da pilha
```



Passagem de parâmetros pela pilha

- Diferentes linguagens de alto nível podem utilizar diferentes regras para empilhar os parâmetros.
- Em C, os parâmetros são empilhados na ordem inversa em que foram declarados.
- Para o procedimento `param_c` declarado como

```
void param_c(int x, int y)
```

a chamada

```
param_c(a, b)
```

seria implementada como mostrado a seguir.

Passagem de parâmetros pela pilha

```
...
ldr   r0,b          @ último parâmetro declarado
push  r0            @ é o primeiro a ser empilhado
ldr   r0,a          @ primeiro parâmetro declarado
push  r0            @ é o último a ser empilhado
bl    param_c       @ faz a chamada
add   sp,8          @ retira os dois parâmetros da pilha.
...
```

Retorno de valores de funções

- No caso de funções (procedimentos que retornam valores), o valor ou valores podem ser retornados em registradores ou na pilha.
- C permite que apenas tipos escalares sejam retornados por funções, e nesse caso um registrador específico é utilizado.
- Algumas linguagens de programação permitem que funções retornem valores de tipos não escalares, e nesses casos a convenção de passagem de parâmetros utiliza outros registradores ou a pilha.
- Em linguagem de montagem podemos fazer as nossas próprias convenções para o retorno de valores por funções, e registradores são a primeira opção.

Problema

Escreva uma função `multiplica` que calcula o resultado da multiplicação de dois números inteiros pelo método de adições sucessivas. Os dois operandos são passados nos registradores `r1` e `r2`, e o resultado deve ser retornado no registrador `r0`.

Solução

```
@ **********
@ multiplica
@ **********

multiplica:
     cmp   r1,r2          @ para minimizar os passos da multiplicação
     bcc   mult1          @ usa menor valor para controlar repetição
     mov   r0,r1          @ troca valores de r1 e r2 usando
     mov   r1,r2          @ r0 como temporário
     mov   r2,r0
mult1:
     mov   r0,#0          @ inicializa valor do produto
mult2:
     sub   r2,#1          @ vamos realizar r2 adições
     bcs   mult3          @ desvia se terminamos
     add   r0,r1          @ adiciona mais uma parcela
     b     mult2
mult3:
     bx    lr             @ retorna quando todas as adições terminaram
```

Problema

Escreva uma função `conta_uns` que devolve em `r0` o número de bits 1 de uma palavra de 32 bits passada como parâmetro pela pilha.

Solução

```
@ *********
@ conta_uns
@ *********
@ Conta o número de bits 1 de uma palavra passada pela pilha
@   entrada: palavra de 32 bits passada pela pilha
@   saída: número de bits 1 em r0
@   destrói: r1 e flags

conta_uns:
     ldr   r1,[sp,#4]      @ carrega parâmetro
     eor   r0,r0           @ zera registrador resultado
proxbit:
     shr   r1,#1           @ testa mais um bit
     bcc   testafim        @ bit deslocado é 1?
     add   r0,#1           @ conta este bit (note que flag Z nunca é um)
testafim:
     bne   proxbit         @ se não verificou todos os bits, continua
     bx    lr              @ retorna com valor em r0
```

Problema

Escreva uma função `compara_uns` que verifica se duas palavras de 32 bits passadas como parâmetro na pilha têm ambas o mesmo número de bits 1. Caso tenham, o registrador `r0` deve retornar com o número de bits 1 contido em cada palavra. Caso contrário, `r0` deve retornar com o valor -1.

Tentativa de solução

```
@ ***********
@ compara_uns
@ ***********
@ Compara o número de bits 1 de duas palavras

compara_uns:
     ldr   r0,[sp,#4]      @ carrega primeiro parâmetro
     push  r0              @ empilha como parâmetro para conta_um
     bl    conta_uns       @ conta o número de bits 1 do primeiro
     add   sp,#4           @ retira parâmetro da pilha
     mov   r1,r0           @ guarda resultado intermediário em r1
     ld    r0,[sp,#8]      @ carrega segundo parâmetro
     push  r0              @ empilha como parâmetro para conta_um
     bl    conta_uns       @ conta o número de bits 1 do segundo
     add   sp,#4           @ retira parâmetro da pilha
     cmp   r0,r1           @ compara resultados
     beq   final           @ se iguais retorna, r0 com num. bits 1
     mov   r0,#-1          @ caso contrário, indica com r0=-1
final:
     bl    lr              @ retorna com valor em r0
```

Tentativa de solução

- a implementação desse exemplo apresenta um problema que ocorre com frequência: como `conta_uns` destrói o registrador `r1`, que é usado em `compara_uns` para guardar o número de bits 1 do primeiro parâmetro, quando `conta_uns` é invocado pela segunda vez, o resultado da primeira chamada, que foi armazenado em `r1`, é perdido.
- Uma solução óbvia para este problema: utilizar outro registrador para armazenar o resultado da primeira chamada.
- No entanto, nem sempre há outro registrador disponível.

Tentativa de solução

- outra solução é geralmente utilizada: o uso da pilha para armazenamento temporário de valores.
- antes da chamada do procedimento os valores dos registradores que se deseja preservar devem ser empilhados
- após o retorno do procedimento os registradores devem ser restaurados com os valores anteriores, armazenados na pilha

Passagem de parâmetros por referência e por valor

- Em linguagens de alto nível o compilador cuida de tratar corretamente esses dois tipos de parâmetros.
- Em linguagem de montagem, o controle é feito exclusivamente pelo programador.

```
exemplo_valor_ref(&ref, 'a', val);
```

Passagem de parâmetros por referência e por valor

```
ldr  r0,=val            @ empilha valor do terceiro parâmetro
ldr  r0,[r0]            @ empilha valor do terceiro parâmetro
push r0                 @ valor contido no endereço val é empilhado
mov  r0,#0x61           @ empilha segundo parâmetro
push r0                 @ valor da constante 'a' é empilhado
ldr  r0,=ref            @ empilha endereço do primeiro parâmetro
push r0                 @ o endereço do rótulo ref é empilhado
bl   exemplo_valor_ref  @ chama o procedimento
add  sp,#12             @ desempilha parâmetros
```

Problema

Traduza para linguagem de montagem do ARM o procedimento `troca`, declarado no Exemplo 3 no início deste capítulo, para trocar os valores de duas variáveis inteiras passadas como referência pela pilha.

```
int x,y,z; // declaração de algumas variáveis

void troca(int *a, int *b) {
    int tmp;

    tmp = *a;
    *a = *b;
    *b = tmp;
}

int main(void) {
    ...
    troca(&x,&y);
    z=x+1;
    troca(&z,&x);
    x=y-1;
    ...
}
```

Solução

```
@ *****
@ troca
@ *****
@ Troca os valores de duas variáveis passadas por referência na pilha
@   entrada: dois endereços de variáveis inteiras, pela pilha
@   saída: nenhuma
@   destrói: r0,r1,r2,r3

troca:
     ldr    r0,[sp,#4]      @ carrega endereço da variável a
     ldr    r1,[sp,#8]      @ carrega endereço da variável b
     ldr    r2,[r0]         @ valor da variável a
     ldr    r3,[r1]         @ valor da variável b
     str    [r0],r3         @ armazena valor de b no endereço de a
     str    [r1],r2         @ armazena valor de a no endereço de b
     ret
```

Solução

Exemplo de chamada:

```
    ...
    ldr   r0,=y          @ carrega endereço da variável y
    push  r0             @ empilha argumento
    ldr   r0,=x          @ carrega endereço da variável x
    push  r0             @ empilha argumento
    bl    troca          @ faz a chamada
    add   sp,#8           @ retira os dois argumentos da pilha
    ...
@ aqui estão definidas as variáveis inteiras
x:   .skip    4
y:   .skip    4
```

Variáveis locais a procedimentos

- Uma variável declarada no corpo de um procedimento é chamada de variável *local* ao procedimento.
- Uma variável local é visível e acessível apenas dentro do corpo do procedimento em que é declarada.
- Registradores são normalmente usados para representar variáveis locais a um procedimento.
- Se o número de registradores não é suficiente para alocar as variáveis de um procedimento, ou se o procedimento é recursivo, as variáveis locais devem ser alocadas na pilha.

Variáveis locais a procedimentos

- A alocação de espaço na pilha para variáveis locais deve ser feita no corpo do procedimento (normalmente na entrada).
- O espaço deve ser desalocado antes do retorno do procedimento. Esse tipo de alocação de espaço para variáveis é denominado de alocação *dinâmica* de variáveis porque, em contraste com a alocação estática, o espaço é alocado apenas quando necessário.

Variáveis locais a procedimentos

- Para alocar espaço na pilha, basta decrementar o número de bytes desejado do registrador `sp`.
- Ao reservarmos espaço para variáveis locais na pilha dentro de um procedimento, o deslocamento necessário, em relação a `sp`, para acessar os parâmetros do procedimento se altera.
- Exemplo: apesar de o endereço normal para acessar o primeiro parâmetro ser `sp+4`, se alocarmos duas palavras para variáveis locais na pilha esse endereço passa a ser `sp+12`.

Registrador apontador de quadro

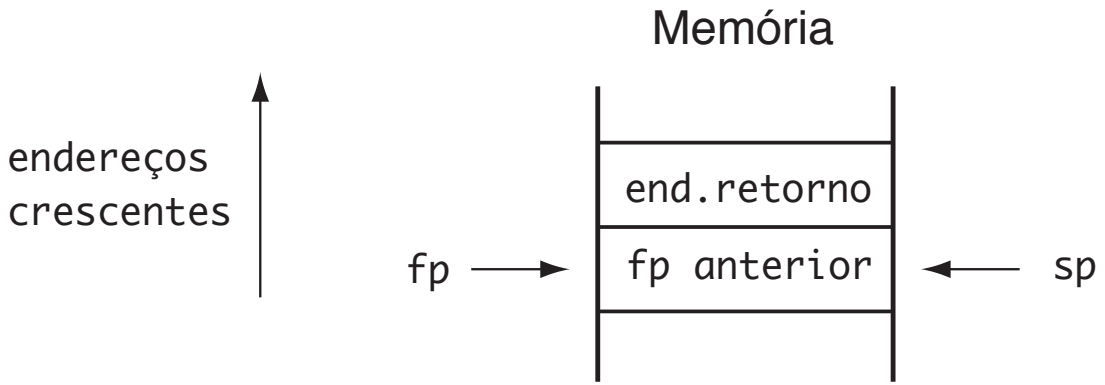
- Para evitar que os deslocamentos sejam alterados durante a execução do procedimento, gerando confusão, é comum utilizarmos mais um registrador, geralmente chamado apontador de quadro (em inglês, *frame pointer*), que é mantido fixo durante a execução do procedimento, apontando para o endereço que `sp` aponta no início do procedimento.
- Os deslocamentos dos parâmetros em relação ao registrador apontador de quadro mantêm-se fixos durante toda a execução do procedimento.
- No ARM, o registrador `r11` pode ser usado como apontador de quadro, e a linguagem de montagem aceita o nome `fp` como sinônimo de `r11`.

- No início do procedimento devemos preparar o uso do apontador de quadro, copiando o valor do apontador de pilha.
- Como o apontador de quadro pode estar sendo utilizado (provavelmente em uma invocação anterior de procedimento), é necessário preservar o seu valor, empilhando-o.

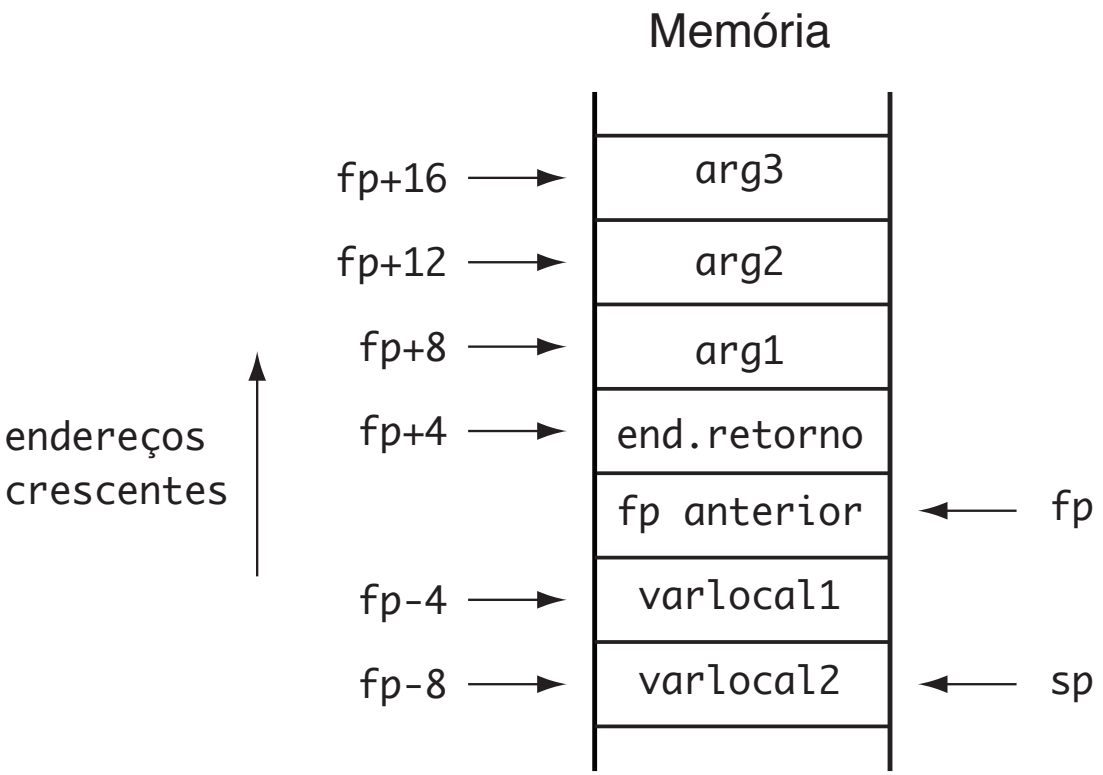
Registrador apontador de quadro

```
     ...
procedim:
     push  fp,lr          @ preserva valor anterior de fp e do endereço de r
     mov   fp,sp          @ e faz cópia do apontador da pilha corrente
     ...
```

Registrador apontador de quadro



Registrador apontador de quadro



Registrador apontador de quadro

```
compara_uns:
     push  fp,lr          @ prepara apontador de quadro
     mov   fp,sp
     sub   sp,#4          @ reserva espaço para variável local i
     ldr    r0,[fp,#8]    @ carrega primeiro parâmetro
     push  r0             @ empilha como parâmetro para conta_uns
     bl    conta_uns      @ conta bits 1 do primeiro parâmetro
     add   sp,#4          @ retira parâmetro da pilha
     str   r0,[fp,#-4]    @ guarda resultado na variável local i
     ldr   r0,[fp,#12]    @ carrega segundo parâmetro
     push  r0             @ empilha como parâmetro para conta_uns
     bl    conta_uns      @ conta bits 1 do segundo parâmetro
     add   sp,#4          @ retira parâmetro da pilha
     ldr   r1,[fp,#-4]    @ recupera resultado da primeira chamada
     cmp   r0,r1          @ compara resultados
     beq   final          @ se iguais retorna, r0 com num. bits 1
     mov   r0,#-1         @ caso contrário, indica com r0=-1
final:
     mov   sp,fp          @ desaloca variável local e
     pop   fp,lr          @ desfaz apontador de quadro, recupera endereço de
     bx    lr             @ retorna com valor em r0
```

Recursão

- Recursão é um conceito muito importante em programação, sendo útil quando a solução de um problema depende da solução de instâncias menores do mesmo problema.
- Agora que sabemos como utilizar a pilha para passar parâmetros e guardar variáveis locais, podemos escrever procedimentos recursivos em linguagem de montagem.

Fatorial

Um exemplo muito comum quando estudamos recursão é o cálculo do fatorial de um número inteiro positivo n, definido como o produto de todos os números inteiros positivos menores ou iguais a n:

$$fatorial(n) = \begin{cases} 1 & se\ n \leq 1 \\ n \times fatorial(n-1) & se\ n > 1 \end{cases}$$

Problema

Traduza a implementação recursiva de fatorial na linguagem C, dada a seguir, para linguagem de montagem do ARM.

```
int fatorial(int n)
{
    if (n<=1)
        return 1;
    else
        return n*fatorial(n-1);
}
```

Solução

```
@ ********
@ fatorial
@ ********
fatorial:
     push  lr
     ldr   r0,[sp,#4]       @ valor de n
     cmp   r0,#1            @ n<=1?
     bhi   fat1             @ se não, desvia para calcular fatorial
     mov   r0,#1            @ valor de fatorial é 1
     pop   lr               @ recupera endereço de retorno original
     bx    lr               @ retorna fatorial(0) ou fatorial(1)
fat1:
     sub   r0,#1            @ calcula recursivamente fatorial(n-1)
     push  r0               @ empilha parâmetro
     bl    fatorial         @ chama recursivamente
     add   sp,#4            @ retira parâmetro da pilha
                            @ neste ponto, r0 tem valor de fatorial(n-1)
     ld    r1,[sp,#4]       @ recupera novamente valor de n
     mov   r2,r0            @ copia fatorial(n-1) em r2
     bl    multiplica_otim  @ efetua r0 <- r1*r2
     pop   lr               @ recupera endereço de retorno original
     bx    lr               @ retorna, r0 tem valor de fatorial(n)
```