Exercícios - Parte D

Exercício 1

Quando o processador entra em modo Handler ele salva o contexto através do salvamento de registradores na pilha. A ordem salvamento é:

XPSR, LR, PC, R12, R3, R2, R1, R0

Sabemos que o processador está em modo Handler pela análise 2 registradores: ISPR e LR. Temos ISPR = 0x0f, o que significa que a exceção de número 0x0f está sendo tratada. Se nenhuma exceção estivesse sendo tratada, este valor seria simplesmente 0x00. O valor de LR = 0xfffffff9 significa que o processador está em modo Handler usando a pilha MSP e deverá retornar ao modo Thread utilizando a pilha MSP, logo significa que está em modo Handler.

Exercício 2

É esperado que ocorram alterações no registrador FPCA do CONTROL. Este registrador indica se no contexto atual o ponto de flutuação está ativo ou não.

Durante a execução do código realmente foi observado o valor 1 no FPCA, indicando que houve ativação do ponto de flutuação. Na imagem o registrador FPCA está 0, porém na cor vermelha, que indica mudança do valor. Sabemos que no momento que a imagem foi capturada, uma exceção estava sendo tratada pelo registrador ISPR, portanto estamos no modo Handler. Neste momento o registrador LR está 0xfffffffe9, indicando que o processador está no modo Handler usando a pilha MSP com estado de ponto flutuante ativo e irá retornar ao modo Thread utilizando a pilha MSP.

Registrador ICSR (Interrupt control and state register): Aciona e limpa o status de exceção do sistema (incluindo Systick), PendSV e NMI). NMI : Non-Maskable Interrupt.

Quando o bit NMIPENDSET foi ativado, o registrador LR passou a ter o valor 0xfffffff1, que significa que o processador irá para o modo Handler, indica que a pilha MSP com ponto flutuante ativo estava sendo usado, e que irá passar a usar a pilha MSP sem o ponto flutuante ativo. Já o registrador CONTROL está zerado, indicando que a flag de ponto flutuante de está desativada. Com isso vemos que o sistema está se preparando para tratar uma exceção de estado de ponto flutuante desativado. Também observamos que o código assembly fez um salto (B) para o endereço 0xc36, onde provavelmente é o handler da exceção NVI. Também vemos que o número da exceção em ISPR é 0x02, o que é o código da ISR NVI, de prioridade -2.

Exercício 3

No exercício 3 foi observado que a pilha que o processador utiliza no modo handler é a PSP, que não pode ser observada pela aba de Stack, somente pelo endereço de memória (por algum motivo). Podemos observar que o valor de LR é de 0xfffffed, que significa que no modo Handler, durante o tratamento da interrupção, o estado de ponto flutuante estava ativo utilizando a pilha PSP, e que o processador irá retornar ao modo Thread, também utilizando a PSP. Da mesma forma que ocorreu com o exercício 2, ao alterar o bit

NMIPENDSET, observamos que o processador foi tratar a interrupção NMI, tendo LR 0xfffffff1, ISPR 0x02. O registrador CONTROL está zerado.