EE 309 - Assignment 3

Prasann Viswanathan, 190070047

Q-1) a)

SP contains DF20.Also, In 8086 the stack grows downward. For every PUSH instruction SP is decremented by 2 (Each count is a byte and we add words which is why 2) and then the value is pushed using the new SP address. The calling function first pushes the arguments of the called function onto the stack.

DF1F & DF20 store S2 start address

DF1D & DF1E store S1 start address

DF1B & DF1C store N

After this SP stores DF1B and assembly level CALL is executed which pushes the return address i.e. the value of IP onto the stack.

DF19 & DF1A contain the return address.

Next we push BP onto the stack so

DF17 & DF18 contain the original Base Pointer value, in order to preserve it.

This completes the stack frame and the called function is ready to execute its body

Q-1) b) code

Q-1) c)

If the number of arguments is fixed and known, then the expression in the instruction “RET expression”, is a 16-bit number depending upon the number of arguments, and it is added to SP after the return address has been popped. This effectively removes any arguments for the called function that had been placed on the stack.

Since it is a requirement that the expression in the instruction “RET expression” must evaluate to a constant at compile time, it is not possible to use this in functions which have a variable number of arguments (like printf).