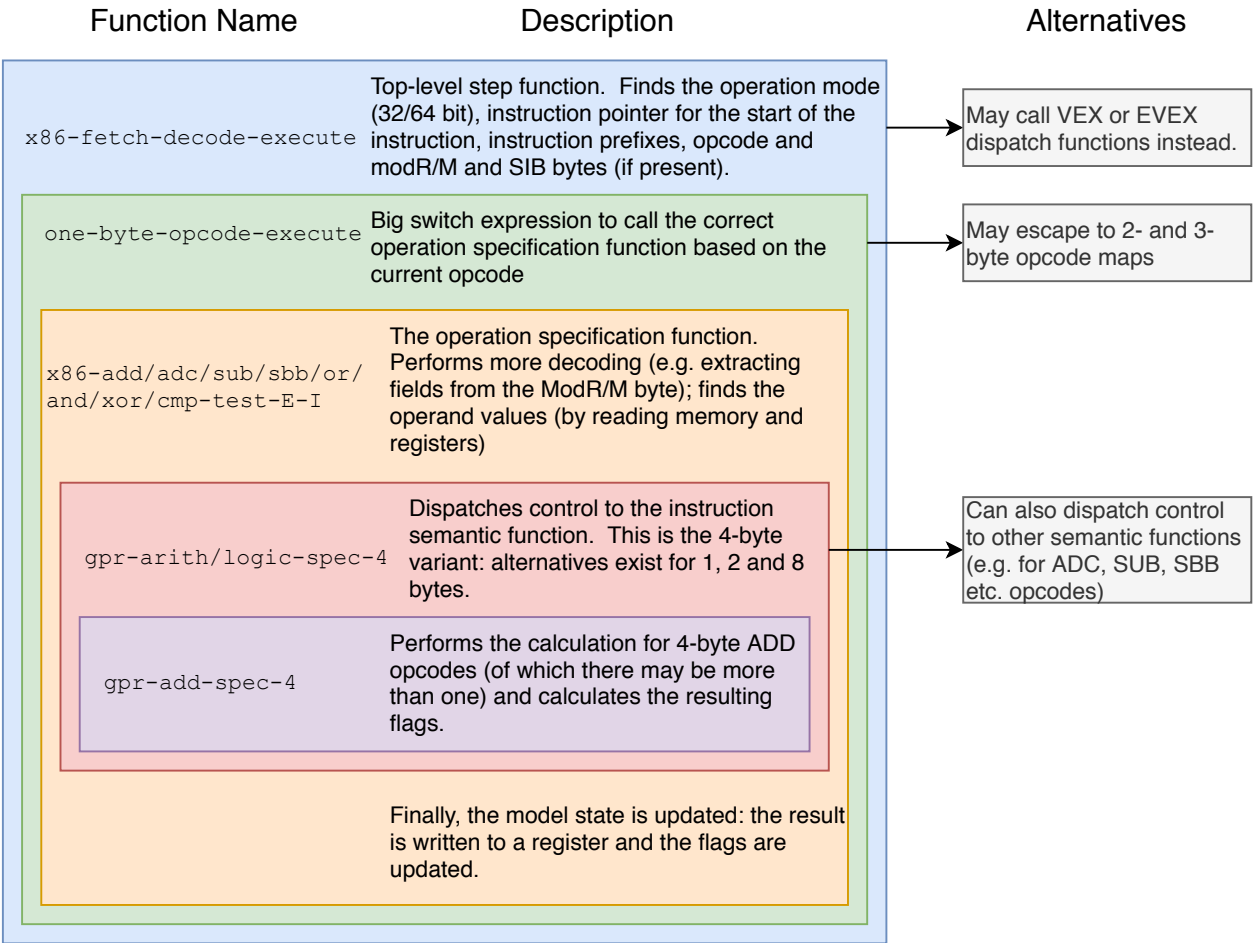
Function Name
Description
Alternatives
x86-fetch-decode-execute
Top-level step function. Finds the operation mode (32/64 bit), instruction pointer for the start of the instruction, instruction prefixes, opcode and modR/M and SIB bytes (if present).
May call VEX or EVEX dispatch functions instead.
one-byte-opcode-execute
Big switch expression to call the correct operation specification function based on the current opcode
May escape to 2- and 3-byte opcode maps
x86-add/adc/sub/sbb/or/and/xor/cmp-test-E-I
The operation specification function. Performs more decoding (e.g. extracting fields from the ModR/M byte); finds the operand values (by reading memory and registers)
gpr-arith/logic-spec-4
Dispatches control to the instruction semantic function. This is the 4-byte variant: alternatives exist for 1, 2 and 8 bytes.
Can also dispatch control to other semantic functions (e.g. for ADC, SUB, SBB etc. opcodes)
gpr-add-spec-4
Performs the calculation for 4-byte ADD opcodes (of which there may be more than one) and calculates the resulting flags.
Finally, the model state is updated: the result is written to a register and the flags are updated.