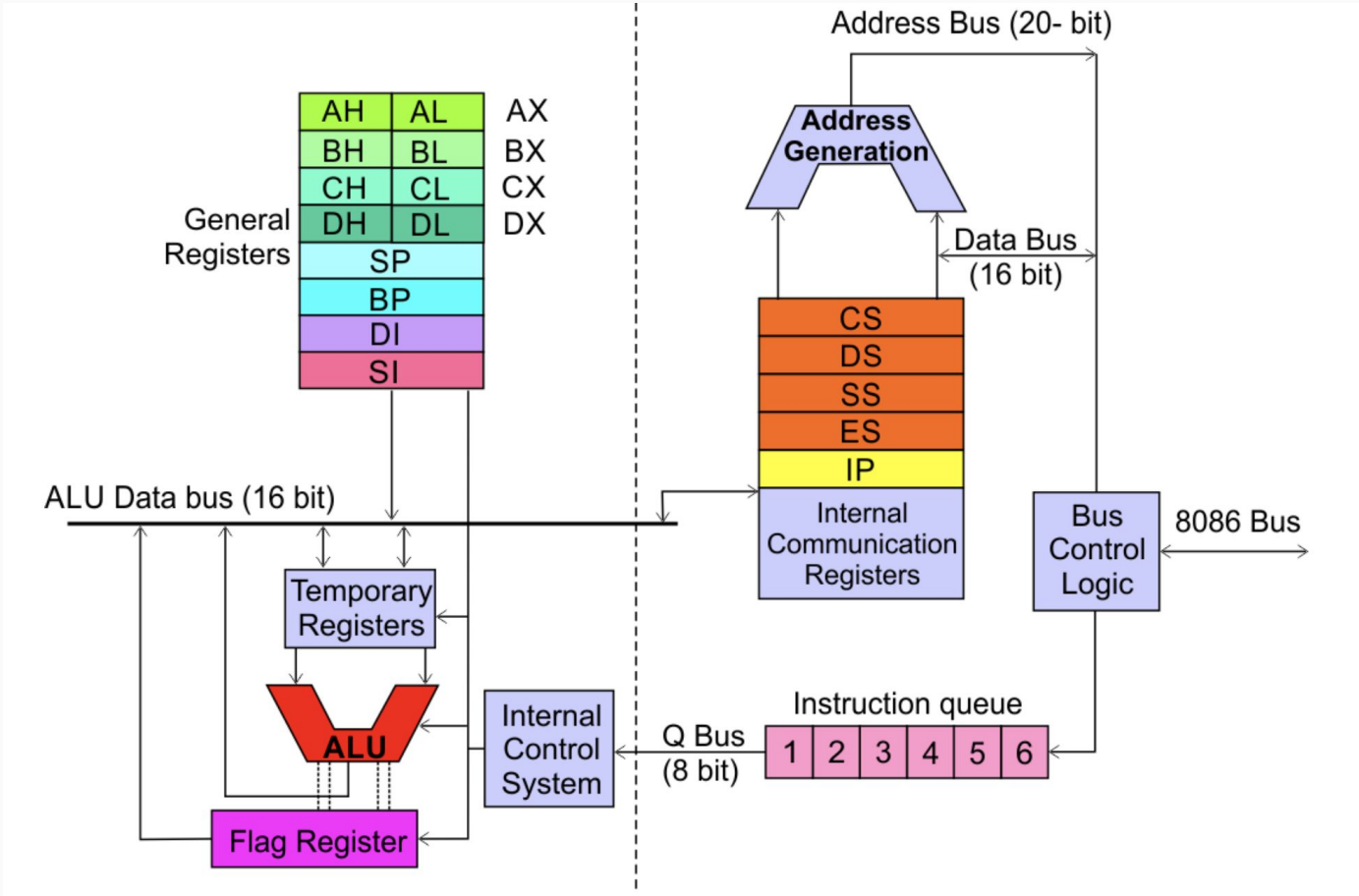
Assembly

Instruction Set - Strings


Address Bus (20- bit)
AH
AL
AX
BH
BL
BX
CH
CL
CX
DH
DL
DX
General Registers
SP
BP
DI
SI
Address Generation
Data Bus (16 bit)
CS
DS
SS
ES
IP
Internal Communication Registers
Bus Control Logic
8086 Bus
ALU Data bus (16 bit)
Temporary Registers
ALU
Internal Control System
Q Bus (8 bit)
Instruction queue
1
2
3
4
5
6
Flag Register

Unsigned/Signed Arithmetic

IMUL / IDIV → Signed

MUL / DIV → Unsigned

ADD/SUB → Always signed

Multiplication

Cases:

- 8-bit x 8-bit → Result in (AX)
- 16-bit x 8-bit → Result in (DX | AX)
- 16-bit x 16-bit → Result in (DX | AX)

AAM → Unpacked Decimal

Division

Cases:

- 8-bit / 8-bit → Quotient in (AL) | Remainder in (AH)
- 16-bit / 8-bit → Quotient in (AX) | Remainder in (DX)
- 16-bit / 16-bit → Quotient in (AX) | Remainder in (DX)

AAD → Unpacked Decimal

LOOP

- What happens when we do the following
  - BACK: MOV CX,0
  - LOOP BACK

- CX is decremented to FFFF
- Infinite loop

String Operations

- Instructions
  - MOVS: Movement
  - CMPS: Comparison
  - SCAS: Scan
  - LODS / STOS: Load and Store
- Rules
  - SI / DI are updated ⇒ Depending on DF
  - Instructions have two formats ⇒ SB / SW

Repeat

- The REP instruction
  - REPZ / REPE
  - REPNZ/ REPNE
- Updates the CX register for count