1 Spruenge und Unterprogrammaufrufe

1.1 Unbedingte Spruenge

"JMP n" (n := Label) Befehl → Sprung an vorgegebene Stelle im Programm

1.2 Bedingte Spruenge

- Sprung erst durch erfuellte Bedingung
- Bedingung orientiert sich an gesetzte Flag im Statusregister die man betrachtet
- die jeweilige Flag (jeweils ein Bit) werden von bestimmten Operationen gesetzt

1.2.1 Statusregister des 80386

wichtigste Register:

Kurzname	Name	Beschreibung
CF	Carry flag	Uebertrag
ZF	Zero flag	Ergebnis ist null
SF	Sign flag	Vorzeichen
DF	Direction flag	Richtung fuer Stream Operation
OF	Overflow flag	Ueberlauf

- bestimmte Befehle aendern nicht die Flags (MOV / PUSH / POP / JMP / CALL / RET)
- bestimmte Befehle koennen Flags aktualisieren / aendern (ADD / SUB / MUL / IMUL / DIV / IDIV / INC / DEC / NEG)

→ DEC / INC manipulieren die Carry Flag nicht
→ getriggerte Flag: Bit wird auf 1 gesetzt
→ Compare Befehl: "CMP" (setzt Flags) → Conditional Jump als Folge
→ "J[cc] n" (n := Label)

[cc] Platzhalter	Beschreibung	Flags
C	carry	CF = 1
NC	no carry	CF = 0
E, Z	equal / zero	ZF = 1
NE, NZ	not equal / not zero	ZF = 0
O	(signed) overflow	OF = 1
NO	(signed not overflow	OF = 0
G, NLE	(signed) greater / not less or equal	((SF xor OF) or ZF) = 0
GE, NL	(signed) greater or equal / not less	(SF xor OF) = 0
L, NGE	(signed) less / not greater or equal	(SF xor OF) = 1
LE, NG	(signed) less or equal / not greater	((SF xor OF) or ZF) = 1

1.3 Unterprogramme

Beim Aufruf eines Unterprogramms durch "CALL" wird die Ruecksprungadresse gesichert um an die geeignete Stelle nach Ausfuehrung des Unterprogramms zurueckzuspringen.

Eventuell werden Daten bei einem Unterprogramm Aufruf durchgegeben
→ ein Unterprogramm kann wie eine Methode fungieren

- erste vier Parameter werden durch EAX / EBX / ECX / EDX uebergeben
- alle weiteren Parameter liegen auf dem Stack

→ Problem: ESP kann variieren, falls das Unterprogramm Daten auf den Stack legt oder vom Stack nimmt

→ Loesung: EBP sichert die Basisadresse zu Beginn des Unterprogramms durch PUSH (muss aber auch wieder gepopt werden)

- "[ebp]": 32Bit Ruecksprungadresse
- "[ebp + 4]": 32Bit Backup von ebp Register
- "[ebp + 8]": Zugriff auf ersten Stackparameter

- jedes Unterprogramm muss alles vom Stack nehmen was es auf den Stack gelegt hat

1.3.1 Calling Convention

- unterschiedliche Konventionen nach Hardware und Software
- Unterprogramme muessen dokumentieren wie sie Parameter erwarten
- Hochsprachencode erwartet Parameter in bestimmter Reihenfolge

1.3.2 Lokale Variablen

- "SUB esp, n" (n := Wert in Bytes)
  → "Platzmachen" fuer Variablen mit insgesamt n Bytes Groesse

- "ADD esp, n" (n muss dabei genauso gross sein wei bei "SUB esp, n")
  → Aufraeumen des genutzten Platzes (Zuruecksetzen)