Dr. Hans Hehl

Austausch illegaler Z80-Befehle

Ersatzroutinen für die Basic-Interpreter XITAN und HEBAS

In vielen Z80-Programmen werden illegale Befehle verwendet. In Z80-Emulationsprogrammen und bei der neuen CPU 64180 können diese Befehle jedoch nicht verwendet werden. Unser Autor zeigt hier am Beispiel der Basic-Interpreter XITAN und HEBAS, wie diese illegalen Z80-Befehle ersetzt werden können. Ebenso wird ein neuer Basic-Befehl USER für den mc- und den NDR-Klein-Computer vorgestellt.

```
alte Folge:                          neue Folge:

28E1  4E       LD C,(HL)             28E1  4E       LD C,(HL)
      DD 69    LD LX,C                     23       INC HL
      23       INC HL                      46       LD B,(HL)
      4E       LD C,(HL)                   C5       PUSH BC
28E6  DD 61    LD HX,C               28E5  DD E1    POP IX
      23       INC HL                      23       INC HL
                                           00       NOP
28E9  4E       LD C,(HL)             28E9  4E       LD C,(HL)
```

Bild 1. Sechs Bytes werden ab der durch das HL-Register angegebenen Speicherstelle in die Register DE, IX und BC kopiert

```
alt:                                 neu:

25C3  DD 7C    LD A,HX               25C3  E5       PUSH HL
      1F       RRA                         DD E5    PUSH IX
      DD 67    LD HX,A                     E1       POP HL
      DD 7D    LD A,LX                     CD 40 47 CALL 4740
      1F       RRA                         E1       POP HL
      DD 6F    LD LX,A                     00 00    NOP NOP
25CD  CB 1A    RR D                  25CD  CB 1A    RR D

                                     ****************************
                                     4740  CB 1C    RR H
                                           CB 1D    RR L
                                     4744  E5       PUSH HL
                                     4745  DD E1    POP IX
                                     4747  C9       RET
```

Bild 2. Diese Routine verändert Low- und High-Byte der Register BC, DE und IX durch den Befehl RRA

```
alt:                                 neu:

26BC  DD 7C    LD A,HX               26BC  E5       PUSH HL
      1F       RRA                         DD  E5   PUSH IX
      DD 67    LD HX,A                     E1       POP HL
      DD 7D    LD A,LX                     CD 40 47 CALL 4740
      1F       RRA                         E1       POP HL
      DD 6F    LD LX,A                     00 00    NOP NOP
26C6  CB 1C    RR H                  26C6  CB 1C    RR H
```

Bild 3. Bei der Multiplikationsroutine finden sich ähnliche illegale Opcodes wie in Bild 2. Es kann der gleiche Einsprung bei 4740H verwendet werden

Im mc 1/82 wurden 422 neue Z80-Befehle veröffentlicht, welche durch eifriges Experimentieren gefunden wurden. Diese Befehle waren jedoch bereits auf einem anderen Kontinent bekannt und wurden dort auch verwendet. Damit stehen 1116 Befehle der Z80-CPU zur Verfügung. Besondere Bedeutung erlangen die zusätzlichen Befehle für die einzelnen Hälften der Indexregister IX und IY. Diese werden so zu vollwertigen Registerpaaren wie die Register HL, DE, oder BC.

Ein Beispiel soll dies erläutern, genauere Hinweise sind in [1] zu finden. Der 8-Bit-Ladebefehl LD C,H (4C) des HL-Registers lautet für das IX-Register LD C,HX (DD 4C). HX steht für die Bits 8...15 von IX. Damit wird das High-Byte des IX-Registers nach Register C kopiert. Entsprechend gibt es zum Befehl LD C,L (4D) den illegalen Teil LD C,LX (DD 4D), wobei LX für die Bits 0...7 steht. Als Ergänzung zu dem in [1] aufgeführten Artikel seien die beiden illegalen Befehle OR HX (DD B4) und OR LX (DD B5) des IX-Registers nachgetragen.

Assembler und Emulatoren steigen aus

Ein großer Nachteil bei der Verwendung der illegalen Befehle besteht darin, daß Hilfsprogramme wie DDT, DDTZ und viele Assembler diese Befehle nicht beherrschen und meistens nur mit einem erstaunten ??? reagieren. Bei einem Debugger kann man sich mühsam durch Setzen von Breakpoints behelfen. Bei Assemblern müssen die Befehle per Byte-Definition direkt gesetzt werden.

Die günstige Preisentwicklung bei Speicherbausteinen und die Entwicklung von 16-Bit- bzw. 32-Bit-CPUs lassen das Arbeitspferd Z80 zunehmend in den Hintergrund treten.

Doch so mancher Umsteiger von CP/M 2.2 auf CP/M-68k würde seine unter CP/M 2.2 erstellten Basic-Programme gerne weiter verwenden. Dazu gibt es einen Z80-Emulator der Firma Soft-Design [2], der auf jedem CP/M-68k-System ein CP/M-80-System Vers. 2.2 nachbildet [3]. Leider werden aber die illegalen Z80-Befehle vom Emulator nicht akzeptiert. Gleiches gilt für die Nachfolger des Z80, z.B. für die CPU 64180, die 512 KByte direkt adressieren kann.

XITAN und HEBAS werden „akzeptabel"

Bei den Basic-Interpretern XITAN von Neil Colvin und dem verbesserten Nachfolger HEBAS (Franzis-Software-Service

und Firma Graf, Kempten) kann man die illegalen Opcodes durch legale ersetzen. Nun laufen auf dem 680XX-NDR-System mit Z80-Emulator beide Interpreter mit den schon vorhandenen Basic-Programmen. Auch die neue CPU-64180-Baugruppe der Fa. Graf macht keine Schwierigkeiten bei den angegebenen Basic-Interpretern.
Ein Nachteil sei nicht verschwiegen. Es können die Speicherbereiche über 64 KByte nicht angesprochen werden, da der Befehl LD (nn),HL (22 XXXX) nur FFFFH als höchste Adresse ansprechen kann. Das gilt auch für CP/M 2.2.
Für die Programmteile des Interpreters, welche die illegalen Opcodes enthalten, wird jeweils die Ersatzroutine angegeben. Da diese mehr Platz benötigen, wurde am Ende des Interpreters Platz reserviert, der von Basic-Programmen nicht überschrieben wird. Der Rücksprung aus der Erweiterung zu gleichen Programmteilen erfolgt zunächst mit Relativsprüngen, dann geht es mit RET (C9) zurück ins Hauptprogramm des Interpreters.

Die Änderungen

Im Rahmen dieses Artikels kann keine genaue Erläuterung aller hier geänderter Programmteile erfolgen. Dies ist einer vollständigen Dokumentation des überarbeiteten Interpreters vorbehalten, die als Kurzfassung (ca. 90 Seiten) z. Zt. auf Diskette vom Autor bezogen [4] und als Dokumentation vom Elektronikladen (Detmold) gedruckt erworben werden kann. Bevor jedoch die aufgezeigten Änderungen (*Bilder 1..16*) durchgeführt werden können, muß sowohl bei XITAN als auch bei HEBAS der Inhalt der Adresse 46BAH in A0 47H umgeändert werden. In Adresse 479FH muß dann der Wert 0 enthalten sein. Die Routine in *Bild 2* verändert Low- und High-Byte der Register BC, DE und IX durch den Befehl RRA. Dabei wird der Inhalt des Akkumulators nach rechts verschoben, wobei der Inhalt des Übertragbits nach Bit 7, der Inhalt von Bit 0 ins Übertragsbit geschoben wird.
Bei der Ausgabe einer Zahl muß das interne Format in die ASCII-Darstellung umgewandelt werden (*Bild 5*). Dies geschieht durch wiederholten Abzug der in einer Tabelle abgelegten, elf sedezimalen Konstanten (1 000 000 000 bis 1) von den in den Registern DE, IX und C enthaltenen Werten. Elf Konstanten liegen deshalb vor, da maximal eine elfstellige Zahlenausgabe möglich ist. In Register B wird die ASCII-Zahl, mit 30H beginnend, hochgezählt und dann jeweils in das ASCII-Zahlen-Flag F92H bis F99H

```
alt:                                neu:

2512  DD 4C     LD C,HX        2512  E5         PUSH HL
      DD 7D     LD A,LX              DD E5      PUSH IX
      DD 67     LD HX,A              E1         POP HL
      DD 6A     LD LX,D        2516  CD 48 47   CALL 4748
251A  AF        XOR A          2519  E1         POP HL

                                     ************************

                                4748  4C         LD C,H
                                      7D         LD A,L
                                      67         LD H,A
                                      6A         LD L,D
                                474C  18 F1      JR 4744
```

```
alt:                                neu:

2911  5F        LD E,A         2911  E5         PUSH HL
      DD 67     LD HX,A              CD 4E 47   CALL 474E
      DD 6F     LD LX,A              E1         POP HL
2916  B7        OR A           2916  B7         OR A

                                     ************************

                                474E  5F         LD E,A
                                      67         LD H,A
                                      6F         LD L,A
                                4751  18 F1      JR 4744
```

Bild 4. Illegale Ladebefehle werden ersetzt

```
alt:                                neu:

4287  DD 7D     LD A,LX        4287  D5         PUSH DE
      9E        SBC A,(HL)           DD E5      PUSH IX
      DD 6F     LD LX,A              D1         POP DE
      23        INC HL               7B         LD A,E
      DD 7C     LD A,HX              9E         SBC A,(HL)
      9E        SBC A,(HL)           5F         LD E,A
      DD 67     LD HX,A        428E  CD 53 47   CALL 4753
4292  23        INC HL               D1         POP DE
                                4292  23         INC HL

                                     ************************

                                4753  23         INC HL
                                      7A         LD A,D
                                      9E         SBC A,(HL)
                                      57         LD D,A
                                      D5         PUSH DE
                                4758  18 EB      JR 4745
```

Bild 5. Umwandlung des internen Formats in die ASCII-Darstellung

```
alt:                                neu:

25AC  DD 55     LD D,LX        25AC  E5         PUSH HL
      08        EX AF,AF'            DD E5      PUSH IX
      DD 7C     LD A,HX              E1         POP HL
      DD 6F     LD LX,A              55         LD D,L
      08        EX AF,AF'            6C         LD L,H
      DD 61     LD HX,C        25B2  CD 5A 47   CALL 475A
25B6  0E 00     LD C,0               E1         POP HL
                                25B6  0E 00      LD C,0

                                     ************************

                                475A  61         LD H,C
                                475B  18 E7      JR 4744
```

Bild 6. Die Halb-Bytes der Register BC, IX, und DE werden nach rechts verschoben

```
alt:                                neu:

2693  DD 55     LD D,LX        2693  E5         PUSH HL
      08        EX AF,AF'            DD E5      PUSH IX
      DD 7C     LD A,HX              E1         POP HL
      DD 6F     LD LX,A              55         LD D,L
      08        EX AF,AF'            6C         LD L,H
      DD 61     LD HX,C              CD 5A 47   CALL 475A
      4F        LD C,A               E1         POP HL
269E  C9        RET                  4F         LD C,A
                                269E  C9         RET
```

Bild 7. Dieser Abschnitt ist fast identisch mit dem ab 25ACH

```
alt:                                neu:

24F9  DD 9D     SBC A,LX        24F9  D5        PUSH DE
      DD 6F     LD LX,A               DD E5     PUSH IX
      23        INC HL                D1        POP DE
      7E        LD A,(HL)             9B        SBC A,E
      DD 9C     SBC A,HX              5F        LD E,A
      DD 67     LD HX,A               CD 5D 47  CALL 475D
2503  23        INC HL                D1        POP DE
                                  2503  23        INC HL

                                    ************************

                                475D  23        INC HL
                                      7E        LD A,(HL)
                                      9A        SBC A,D
                                      57        LD D,A
                                      D5        PUSH DE
                                4762  18 E1     JR 4745
```

Bild 8. Von den in den Flags F8AH bis F8EH enthaltenen Werten werden die in den Registern DE, IX und C enthaltenen Werte abgezogen

```
alt:                                neu:

2597  DD 9D     SBC A,LX        2597  D5        PUSH DE
      DD 6F     LD LX,A               DD E5     PUSH IX
      7D        LD A,L                D1        POP DE
      DD 9C     SBC A,HX              9B        SBC A,E
      DD 67     LD HX,A               CD 64 47  CALL 4764
25A0  7D        LD A,L                D1        POP DE
                                  25A0  7D        LD A,L

                                    ************************

                                4764  5F        LD E,A
                                      7D        LD A,L
                                      9A        SBC A,D
                                      57        LD D,A
                                      D5        PUSH DE
                                4769  18 DA     JR 4745
```

Bild 9. Ersatz eines illegalen Subtraktions- und Ladebefehls

```
Test auf den Wert FF bei den Registern DE, IX und BC

alt:                                neu:

2560  DD 2C     INC LX          2560  E5        PUSH HL
      C0        RET NZ                CD 6B 47  CALL 476B
      DD 24     INC HX                E1        POP HL
2565  C0        RET NZ          2565  C0        RET NZ

                                    ************************

                                476B  DD E5     PUSH IX
                                      E1        POP HL
                                      2C        INC L
                                      E5        PUSH HL
                                      DD E1     POP IX
                                      C0        RET NZ
                                      24        INC H
                                4774  18 CE     JR 4744
```

Bild 10. Test auf den Wert FFH bei den Registern DE, IX und BC

```
alt:                                neu:

2578  DD 8D     ADC A,LX        2578  D5        PUSH DE
      DD 6F     LD LX,A               DD E5     PUSH IX
      23        INC HL                D1        POP DE
      7E        LD A,(HL)             8D        ADC A,E
      DD 8C     ADC A,HX              5F        LD E,A
      DD 67     LD HX,A               CD 76 47  CALL 4776
2582  23        INC HL                D1        POP DE
                                  2582  23        INC HL

                                    ************************

                                4776  23        INC HL
                                      7E        LD A,(HL)
                                      8A        ADC A,D
                                      57        LD D,A
                                      D5        PUSH DE
                                477B  18 C8     JR 4745
```

Bild 11. Hier werden die Werte der Flags F8AH bis F8DH zu den Werten der Register DE, IX und C addiert

abgelegt. Dann kann diese Zeichenkette ausgegeben werden.
In *Bild 8* werden von den Werten der Flags F8AH bis F8EH die Werte der Register DE, IX und C abgezogen und die Ergebnisse wieder in den Registern DE, IX und C abgelegt. Das HL-Register dient als Zeiger auf die Flags F8AH bis F8EH. Das Register B wird gesondert behandelt.
In diesem Zusammenhang sei auf das Buch von Röckrath aus der Serie Computerpraxis des Franzis-Verlages [5] verwiesen, das grundsätzliche Erläuterungen der Arbeitsweise von Basic-Interpretern enthält.

Eigene Basic-Erweiterungen

Allerdings soll kurz auf die Möglichkeit eingegangen werden, wie eigene Erweiterungen in Maschinensprache im Interpreter resident abgelegt werden können. Es kann der Speicherbereich nach den Systemmeldungen des Kaltstarts Verwendung finden, der aber nicht von Basic-Programmen überschrieben werden darf. Die Anfangsadresse eines Basic-Programmes steht in Adresse 46BAH. Bei XITAN steht dort 45D8H, bei HEBAS je nach Version eine höhere Adresse, z.B. 4740H. Setzt man bei Adresse 46BAH z.B. den Wert 4900H ein, so werden ab dieser Adresse die Basic-Programme abgelegt. Natürlich verringert sich dadurch der zur Verfügung stehende Speicherplatz. Wichtig ist, daß das Byte vor dem ersten Byte des Basic-Programmes den Wert 0 besitzt. Ein Ausführungsbeispiel für einen neuen Basic-Befehl USER soll dies verdeutlichen.

USER-Befehl unter XITAN- und HEBAS-Basic

Der unter CP/M zur Verfügung stehende USER-Befehl kann mit folgender Änderung auch in Basic anstelle des selten benötigten Basic-Befehls USR als Direktbefehl eingerichtet werden. Der USER-Befehl ermöglicht die Zusammenfassung bestimmter Dateigruppen, z. B. nur Systemprogramme oder nur Basic-Programme in einem eigenen Bereich des Inhaltsverzeichnisses. Sie erscheinen dann beim DIR-Befehl nur nach Umschaltung auf den gewählten User-Bereich. Damit bei beiden Interpretern mit dem DIR-Befehl alle Dateien mit beliebigen Dateizusatz angezeigt werden, müssen ab Adresse 35B9H die drei Bytes 42H, 41H und 53H jeweils durch 3FH ersetzt werden (alte Maske ????????BAS, neue Maske ??????????? beim DIR-Kommando).