Dem Prozessor auf der Spur

Die INPUT 64-Assembler-Schule

Mit unserem neuen Kurs über 6502-Maschinensprache wollen wir Sie aus dem Dunst dieser Gerüchteküche befreien. Steigen Sie ein in die 'Haute Cuisine' der Assembler-Programmierung. Im Verlauf dieses Kurses werden Sie köstliche Rezepte kennenlernen, mit denen Sie Ihren Rechner füttern können. Eine Versuchsküche, in der garantiert nichts anbrennt, liefern wir Ihnen gratis dazu.

Wenn man normalerweise anfängt, sich mit der Maschinensprache zu beschäftigen, ist spätestens nach zwei Wochen ein neuer Reset-Knopf oder gar ein neuer Netzschalter für den Rechner fällig. Ganz abgesehen von den Nerven, die durch ständiges neues Laden von Assembler und Monitor auf eine harte Probe gestellt werden.

Mit der INPUT-Assembler-Schule geht das ganz anders: In dem Programm enthalten ist in jeder Folge ein Editor, mit dem Sie eigene Maschinenprogramme erstellen können. Schon in dieser Phase werden Syntax-Fehler abgefangen. Das selbsterstellte Programm kann dann von dem ebenfalls mitgelieferten Assembler übersetzt werden.

Der eigentliche Clou ist aber der Prozessor-Simulator. Er ermöglicht das Austesten der eigenen Programme unter vollständiger Kontrolle des Rechners. Der Einzelschritt-Modus knackt selbst die hartnäckigste Endlos-Schleife, und kein undokumentierter Opcode kann den Rechner zum Absturz bringen.

Maschinensprache ist unwahrscheinlich kompliziert, schwer zu lernen, Maschinensprache-Programme sind aufwendig zu erstellen, und überhaupt ist Maschinensprache nur etwas für Profis. Diese und andere Vorurteile halten sich immer noch hartnäckig in den Köpfen vieler Computer-Besitzer. Und trotzdem träumt fast jeder davon, diese sagenumwobene Sprache zu lernen, denn überall ist zu hören, daß Maschinensprache die schnellste Programmiersprache überhaupt ist und erst sie die letzten Möglichkeiten des Computers aus ihm herausholt.

Die Flachsprache

Maschinensprache ist die 'Muttersprache' eines jeden Computers. Darum ist sie so schnell. Alle höheren Programmiersprachen wie etwa BASIC brauchen einen Übersetzer, der die Programme für den Prozessor verständlich macht. Auch im C64 läuft ein solcher Übersetzer. Es handelt sich dabei um ein Maschinensprache-Programm (was sonst?), genannt BASIC-Interpreter. Er liest ein BASIC-Programm Befehl für Befehl, entschlüsselt jeden einzelnen und führt die entsprechenden Aktionen aus.

Bei Maschinensprache-Programmen ist das ganz anders: Hier versteht der Prozessor direkt die im Speicher liegenden Befehle. Es ist wohl klar, daß so ein 'fest verdrahteter' Befehls-Ausführer schneller ist als ein Programm, das die Befehle erst in Maschinensprache übersetzen muß.

Andererseits sind die Befehle, die der Prozessor direkt versteht, nicht so leistungsfähig wie beispielsweise BASIC-Befehle. Für ein Maschinensprache-Programm muß man also das zu lösende Problem weiter 'aufdröseln'.

Ausprobieren und Simulieren

Zur Bedienung des Lernprogramms

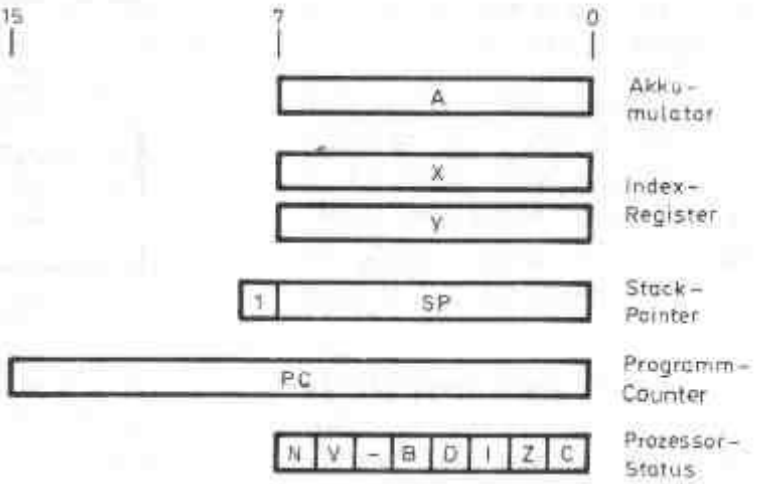
Die INPUT 64-Assembler-Schule setzt sich aus mehreren Teilen zusammen. Nach dem Laden sehen Sie ein Titelbild, von dem aus Sie mit einem beliebigen Tastendruck in das Hauptmenü gelangen.

Wenn Sie nun F1 drücken, gelangen Sie in ein Menü, das Ihnen verschiedene Themen zur Auswahl stellt. Die Erklärungen, die Sie jetzt abrufen können, sollten Sie parallel zum Beiheft lesen. Beide Medien ergänzen sich hier. Sie können die Erklärungen auch mit CTRL-b ausdrucken. Ins Hauptmenü gelangen Sie jederzeit mit der STOP-Taste zurück.

Mit F3 gelangen Sie aus dem Hauptmenü zu einer Auswahl verschiedener Beispielprogramme. Sie können eines davon auswählen, das Sie sich dann im Editor anschauen oder auch verändern können. Wenn Sie an dieser Stelle eine Null eingeben, enthält der

Binär	Dezimal	Hex
0000	0	0
0001	1	1
0010	2	2
0011	3	3
0100	4	4
0101	5	5
0110	6	6
0111	7	7
1000	8	8
1001	9	9
1010	10	A
1011	11	B
1100	12	C
1101	13	D
1110	14	E
1111	15	F

Tabelle 1:
Die Zahlensysteme auf einen Blick



Bis auf den Programmzähler sind die Register des 6510 acht Bit breit. In der ersten Folge der Assembler-Schule beschäftigen wir uns mit dem Akkumulator und einem Flag im Statusregister.

Vokabeln

Wir haben gesagt, daß die Maschinensprache-Befehle so im Speicher liegen, daß der Prozessor sie direkt verstehen kann. Für uns Menschen sind sie aber nur schwer zu merken. Darum hat man die sogenannte Assembler-Sprache entwickelt. Sie besteht aus Befehlen, die sehr eng mit der Maschinensprache in Zusammenhang stehen. Jedem Maschinensprache-Befehl ist eine leicht zu merkende Kombination aus drei Buchstaben - genannt Mnemonic zugeordnet (jawohl, mit 'Mn' - ich habe das Wort nicht erfunden). Wir werden uns in diesem Kurs daher nicht mit der eigentlichen Maschinensprache auseinandersetzen, sondern mit der Assemblersprache.

Es gibt Programme, die ein in Assemblersprache geschriebenes Programm in ein Maschinen-Programm übersetzen. So ein Programm heißt Assembler. Den Text, den es verarbeitet, nennt man Source- oder Quell-Code, das Maschinen-Programm, das er erzeugt, heißt dann Object-Code. Allerdings sollte man diese strenge Begriffstrennung nicht allzu eng sehen. Man spricht oft schon von einem Assembler- oder Maschinen-Programm, wenn man eigentlich den Quell-Code meint. Oft wird auch leichthin behauptet, ein Maschinensprache-Programm sei 'in Assembler geschrieben'.

Von Bits und Bytes

Ein Bit ist die kleinste Informationseinheit eines jeden Digital-Rechners. Man kann sich ein Bit als einen Schalter vorstellen, der entweder offen ist (dann fließt kein Strom, das Bit hat den Wert Null) oder geschlossen (Stromfluß, Wert ist Eins). In solchen Schaltern kodiert jeder Computer seine Programme und Daten. Einen Code mit nur zwei Zuständen nennt man binären oder zweiwertigen Code. Der Name Bit kommt übrigens aus dem

Editor das zuletzt bearbeitete Programm, beim ersten Aufruf ist der Textspeicher leer.

Wenn Sie ein Beispielprogramm bearbeitet haben und - mit der STOP-Taste - wieder ins Hauptmenü springen, können Sie Ihren Text auch auf einen Drucker ausgeben lassen oder auf einen eigenen Datenträger abspeichern. Abgespeicherte Programme können Sie direkt mit dem INPUT-ASS (Ausgabe 6/86) laden und weiterbearbeiten.
Vom Editor aus gelangen Sie mit F7 in einen integrierten Simulator. Hier können Sie unsere Programmbeispiele oder Ihre selbstentworfenen Programme ablaufen lassen und testen, ob sie sich erwartungsgemäß verhalten.

Ausführliche Hinweise zur Bedienung des Editors und des Simulators sind im Programm enthalten. Sie können sie von dort aus jeweils mit der Funktionstaste F6 aufrufen. Es wird empfohlen, diese Seiten vor der Benutzung des Programmpakets einmal gründlich zu lesen. Besitzer eines Druckers können sie auch mit CTRL-b zu Papier bringen.

Englischen und ist die Abkürzung für Binary digiT (binäre Ziffer).

Aus mehreren binären Ziffern kann man eine Zahl bilden. Eine vierstellige Binärzahl (auch Nibble genannt) kann sechzehn verschiedene Werte annehmen. Das zeigt Tabelle 1. Auf die dritte Spalte kommen wir noch zu sprechen.

Man kann mit einem Nibble also die Zahlen Null bis Fünfzehn darstellen. Dabei hat jede Stelle einer Binärzahl den doppelten Stellenwert der rechts von ihr stehenden. In dem Ihnen wahrscheinlich geläufigeren Dezimalsystem, bei dem jede Ziffer zehn verschiedene Werte annehmen kann, hat jede Stelle ja auch den zehnfachen Wert der vorangehenden.

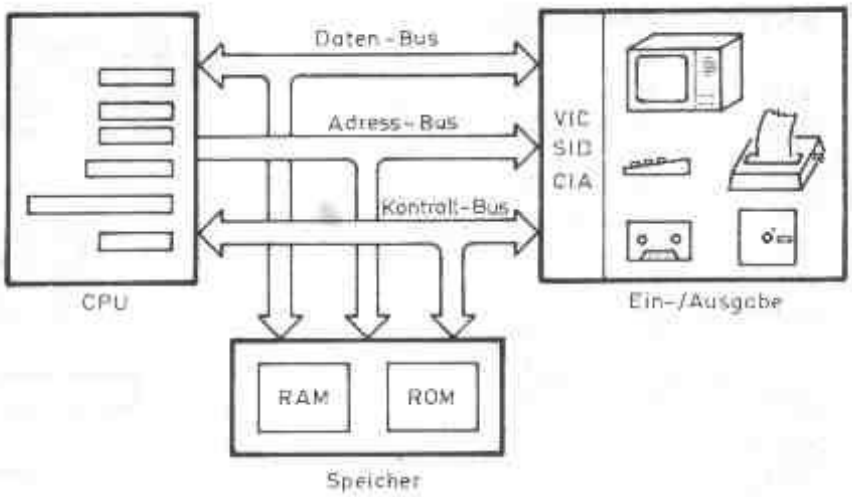
Der Prozessor, der im C64 'tickt', ist ein Acht-Bit-Prozessor. Das heißt, daß er Register (interne Speicherzellen) besitzt, die acht Bits parallel verarbeiten können. Eine solche Binärzahl mit acht Stellen heißt Byte.

Um nicht jedesmal eine achtstellige Binärzahl hinschreiben zu müssen, wenn man ein Byte meint, haben findige Mathematiker das Hexadezimalsystem erfunden. Bei ihm gibt es sechzehn verschiedene Ziffern. Ein Nibble läßt sich also mit nur einer, ein Byte mit zwei Hexadezimalziffern darstellen. Neben den gewohnten Ziffern werden noch die Buchstaben A bis F als Ziffern 'mißbraucht'. Die Zuordnung zeigt Tabelle 1.

Im Hexadezimalsystem hat jede Ziffer den sechzehnfachen Wert der vor ihr stehenden. Mit zwei Nibbles kann man also 16*16, das sind 256 verschiedene Zahlen, darstellen (0 bis 255).

Harte Sachen

Bevor es mit dem Programmieren richtig losgeht, sollen noch einige Begriffe erwähnt werden: Zum Beispiel, daß der Prozessor des C64 den Namen 6510 trägt. Er ist ein Abkömmling der 6502-CPU und versteht die gleichen Befehle wie diese. CPU ist mal wieder eine Abkürzung aus dem Englischen und kommt von 'Central Processing Unit', etwa 'Zentrale Verarbeitungseinheit'. Damit ist auch die Aufgabe eines Prozessors innerhalb eines Computersystems umrissen.



Zu einem Rechner gehören noch die beiden Funktionsblöcke Speicher und Ein-/Ausgabe-Einheit. Mit ihnen steht der Prozessor über elektrische Leitungen in Verbindung, die man Busse nennt. Es gibt einen acht Bit 'breiten' Datenbus, über den die Informationen zwischen den Komponenten ausgetauscht werden, und einen Adreß-Bus, mit dem die CPU dem Speicher mitteilt, welche Speicherstelle gemeint ist. Darüber hinaus gibt es noch Leitungen, die den zeitlichen Ablauf der Aktionen oder die Richtung des Datenflusses bestimmen. Diese Leitungen faßt man zum Kontroll- oder Steuer-Bus zusammen.

Der Adreß-Bus umfaßt beim 6510 sechzehn Leitungen. Damit können zwei hoch sechzehn, das sind 65536 verschiedene Speicherzellen angesprochen werden. Diesen Bereich teilt man in 256 Seiten (Pages) zu je 256 Adressen ein. Wir werden noch sehen, daß einige dieser Seiten für den Prozessor eine besondere Bedeutung haben.

Jedes Computersystem besteht aus drei Komponenten: einer zentralen Verarbeitungseinheit (CPU), einem Speicher und einer Ein-/Ausgabe-Einheit, Den Konakt mit der Außenwelt stellen beim C64 ein Video-Controller, ein Synthesizer-Baustein und zwei universelle Ein-/Ausgabe-Chips her.

Das erste Programm

Jetzt wollen wir aber endlich programmieren! Dabei soll unser Prozessor gleich etwas tun, was man täglich benötigt. Wir wollen ein Programm schreiben, das zwei Zahlen addiert. Der erste Assembler-Befehl, den wir benutzen wollen, heißt

LDA #6

Wie fast alles, was mit Computern zu tun hat und nicht auf Anhieb verständlich ist, handelt es sich um eine englische Abkürzung. Sie steht für 'LoaD Accumulator'. Dieser Befehl dient dazu, eine jener CPU-internen Speicherzellen, die wir Register nennen, mit einem Wert zu füllen. Dieses Register heißt Accumulator (Sammler) oder kurz Akku. Es ist ein sehr wichtiges Register, da es bei allen arithmetischen Operationen beteiligt ist.

Der Prozessor will natürlich noch wissen, welchen Wert er in den Akku laden soll. In unserem Beispiel soll das die Zahl 6 sein. Das Doppelkreuz signalisiert, daß es unmittelbar (immediate) die Zahl 6 sein soll und nicht etwa der Inhalt der Speicherstelle Nummer 6.

Als nächstes soll der Prozessor zu der im Akku gespeicherten Zahl etwas addieren, beispielsweise die Zahl 3. Der Befehl dazu lautet

```
ADC #3
```

und bedeutet 'ADd to accumulator with Carry'. Das Doppelkreuz und die 3 stellen wieder ein unmittelbares Argument dar.

Was soll nun 'with Carry' bedeuten? Dazu muß man wissen, daß es in der CPU ein sogenanntes Statusregister gibt. Eines seiner Bits heißt Carry-Flag. Diese 'Flagge' wird von der CPU unter anderem dann gesetzt, wenn bei einer Addition ein Übertrag entsteht. Übertrag heißt, daß das Ergebnis größer als 255 wurde und somit nicht mehr in ein 8-Bit-Register paßt. Sein Inhalt wird auch bei einer Addition immer noch zum Ergebnis dazugezählt. Wir hätten es darum vor der Addition löschen sollen. Dazu dient der Befehl

```
CLC
```

(CLear Carry flag), den wir also noch vor unser Programm schreiben müssen. Bislang besteht unser Programm also aus den Befehlen

```
CLC
LDA #6
ADC #3
```

Laß' gehn!

Wir wollen uns jetzt auf dem Bildschirm ansehen, wie es arbeitet. Gehen Sie dazu ins Hauptmenü der 'Assembler-Schule', drücken Sie F3 und wählen Programm 1 aus. Sie sehen (hoffentlich) ein Listing unseres ersten Programms. Drücken Sie nun F7. Am oberen Bildschirmrand erscheinen die Zeilen

```
A  X  Y  SP  PC    NV-BDIZC
00 00 00 fe  c000  00110000 clc
```

Ganz links, unter dem A, wird der Inhalt des Akkus (hexadezimal) angezeigt, unter den Buchstaben NV-BDIZC in binärer Form der des Status-Registers. Sein niederwertigstes Bit — unter dem C — ist die Carry-Flagge. Rechts steht der als nächstes auszuführende Befehl. Um ihn ausführen zu lassen, drücken Sie die Leertaste.

An den Register-Inhalten ändert sich dadurch nichts. Die Carry-Flagge war ja schon gelöscht, aber sicher ist sicher.

Nach dem nächsten Druck auf die Leertaste wird der Befehl LDA #6 ausgeführt. Der Akku enthält nun die Zahl 6. Noch mal SPACE - die Addition wird ausgeführt, der Akku enthält nun 9. Die Carry-Flagge zeigt nach wie vor 0 an, ein Übertrag ist ja nicht aufgetreten.

In den Speicher schreiben

Der nächste Befehl, den Sie lernen sollten, heißt

```
STA $C008
```

und bedeutet 'STore Accu', also 'speichere den Inhalt des Akkus ab'. Und zwar in die Speicherstelle, deren Adresse hinter dem Befehl steht. In unserem Beispiel also an die Adresse C008 hexadezimal.

Springen Sie mit F7 wieder in den Editor, schreiben Sie diesen Befehl hinter unser bisheriges Programm und lassen es erneut ausführen. In der zweiten inversen Zeile in der unteren Hälfte des Bildschirms sollten Sie hinter der Adresse $C008 beobachten können, wie der Inhalt des Akkus dorthin kopiert wird.

Sie könnten erneut in den Editor gehen und andere Zahlen hinter die Befehle LDA und ADC schreiben. Die Doppelkreuze sollten Sie aber stehenlassen. Probieren Sie doch mal aus, wie groß die beiden Argumente höchstens sein können, ohne daß nach der Addition die Carry-Flagge gesetzt ist. Wie sieht das Ergebnis aus, wenn ein Übertrag auftritt?

Noch'n Programm

Wenn Sie diese Fragen geklärt haben, laden Sie bitte das zweite Programm in den Editor. (Mit STOP ins Hauptmenü, F3 drücken und 2 wählen.) Dieses Programm soll Ihnen etwas über Programm-Dokumentation zeigen.

Alle Zeilen, die mit einem Semikolon beginnen, enthalten einen Kommentar, der einzig und allein der Lesbarkeit des Programms dienen soll. Sie treten nach der Übersetzung durch den Assembler im eigentlichen Maschinen-Programm nicht mehr in Erscheinung.

Überall, wo in der zweiten Spalte (mit der Überschrift 'labl') etwas steht, wird ein Label definiert. Labels sind symbolische Namen für bestimmte Speicheradressen. Man kann sie auch als Variable für den Assembler auffassen. Sie enthalten als Wert die Adresse, hinter der sie stehen. Überall, wo im Quell-Code beispielsweise das Argument 'SUM1' auftaucht, setzt der Assembler dafür $C014 ein. Der Sinn dieser symbolischen Adressen ist in dem Artikel „Assembler als Hochsprache" an anderer Stelle in diesem Heft ausführlich erklärt.

Doch nun zu dem, was das Programm

tut: Den Befehl CLC kennen Sie schon. Der nächste Befehl heißt

LDA SUM1

SUM1 steht für 'erster Summand'. Dieser Name ist aber völlig beliebig. Er ist wie gesagt nur ein symbolischer Name für die Adresse $C014. Vor diesem Argument steht kein Doppelkreuz. Es handelt sich also nicht um ein unmittelbares Argument. (Die Zahl $C014 würde im übrigen auch gar nicht in den Akku passen.) Diese Adressierungsart heißt 'absolut'. Das bedeutet, der Akku soll mit dem Inhalt der absoluten Adresse $C014 geladen werden.

An der Adresse $C014 steht

W $1234

W ist kein Maschinensprache-Befehl, sondern eine Anweisung für den Assembler. Sie veranlaßt ihn, bei der Übersetzung an diese Adresse die dahinterstehende Zwei-Byte-Zahl zu schreiben. Dabei schreibt er das niederwertige Byte an die angegebene und das höherwertige an die folgende Adresse. Eine Zwei-Byte-Zahl in dieser Form wird auch 'Wort' genannt - daher der Befehl W.

In unserem Beispiel werden also nach der Übersetzung die Speicherstelle $C014 den Inhalt $34 und die Speicherstelle $C015 den Wert $12 haben.

Nach der Ausführung des Befehls 'LDA SUM1' wird der Akku also in unserem Beispiel den Inhalt $34 haben.

Die folgenden Befehle sollten Ihnen keine Rätsel mehr aufgeben: ADC SUM2 addiert den Inhalt der Speicherstelle, die den symbolischen Namen 'SUM2' hat, zum Inhalt des Akkus. STA SUMM speichert den Akku-Inhalt an die Adresse mit dem Label 'SUMM'.

An dieser Adresse taucht eine andere Assembler-Anweisung auf: Der Befehl

S 2

bewirkt, daß der Assembler an dieser Adresse zwei Bytes Platz (Space) läßt. Er füllt diese Adressen mit Null. Diese Adressen können vom Programm als Variable benutzt werden. In unserem Fall nehmen Sie das Ergebnis einer Zwei-Byte-Addition auf.

Der letzte unklare Befehl in diesem Programm ist

BRK

Er bedeutet BReaK (Abbruch). Wenn der Prozessor auf diesen Befehl trifft, hört er mit der Bearbeitung des Programmes auf und springt an eine (hardwaremäßig festgelegte) Adresse. Beim C64 wird dann normalerweise der Bildschirm gelöscht, und in der ersten Bildschirmzeile erscheint die Meldung 'READY.' Innerhalb unseres Simulators wird diese Meldung in der untersten Bildschirmzeile ausgegeben, und Sie können wieder in den Editor oder zum Hauptmenü springen.

Zieh ab!

Im dritten Beispiel-Programm geht es um die Subtraktion. Hier erst mal die neuen Befehle:

SEC

ist die Abkürzung für 'SEt Carry flag' und tut genau das Gegenteil von CLC. Mit diesem Befehl kann - zum Beispiel vor einer Subtraktion - in die Carry-Flagge eine 1 geschrieben werden.

SBC #$82

subtrahiert das Argument vom Inhalt des Akkus. Ausgeschrieben heißt der Befehl 'SuBtract from accu with Carry'. Dabei muß die Carry-Flagge gesetzt sein, sonst wird 'einer mehr' abgezogen. Tritt ein Unterlauf auf, so wird die Carry dabei gelöscht.

Im Prinzip funktioniert eine Subtraktion in Assembler genau wie eine Addition. Man muß nur die Befehle ADC gegen SBC und CLC gegen SEC austauschen.

Das Beispiel-Programm Nummer drei zeigt, wie ein Ein-Byte-Wert von einer Zwei-Byte-Zahl abgezogen wird. Dabei treten in einem Programm verschiedene Adressierungsarten auf — das ist völlig normal, die beiden anderen Programme waren etwas Besonderes.

Der Befehl SBC #0 sieht auf den ersten Blick einigermaßen überflüssig aus, ist er aber nicht. Wenn nämlich in der vorhergehenden Subtraktion vom Low-Byte ein Unterlauf aufgetreten ist, ist die Carry-Flagge an dieser Stelle gelöscht, und es wird nicht Null, sondern Eins vom High-Byte abgezogen. Und genau das ist ja beabsichtigt. Mit diesem 'Trick' sind Ein- und Zwei-Byte-Werte verknüpfbar. Diese Vorgehensweise entspricht dem spaltenweisen Subtrahieren von Dezimal-Zahlen, in der ein Unterlauf ja auch nach links übertragen wird.

Auch bei diesem Programm kann man übrigens die jeweils entgegengesetzten Befehle einsetzen, und es wird addiert. Wenn nämlich bei der Addition auf das niederwertige Byte ein Überlauf entsteht, wird die Carry gesetzt, und der Befehl ADC #0 addiert in Wirklichkeit Eins.

In der nächsten Folge der 'Assembler-Schule' werden Sie unter anderem lernen, wie negative Zahlen in Assembler behandelt werden. HS

Literatur

Christian Persson,
6502/65C02 Maschinensprache,
Verlag Heinz Heise GmbH,
Hannover 1983

Rodnay Zaks,
Programmierung des 6502,
Sybex-Verlag GmbH,
Düsseldorf 1981

Die entscheidenden Sprünge

Zweite Folge der Assembler-Schule

Nachdem in der ersten Folge einige grundlegende Maschinensprache-Befehle gezeigt wurden, befassen wir uns in dieser Folge mit weiteren Arithmetik-Operationen. Neben neuen Befehlen werden Sie die Bits des Statusregisters im einzelnen kennenlernen sowie die Index-Register X und Y benutzen. Wenn Sie diese Folge durchgearbeitet haben, werden Sie außerdem wissen, wie bedingte Programm-Sprünge in Assembler kodiert werden.

Bevor wir aber zu neuen Programmen kommen, wollen wir einen einen kurzen Blick auf die Art und Weise werfen, wie Maschinen-Programme im Speicher abgelegt und vom Prozessor verarbeitet werden.

Ihnen ist sicherlich beim Experimentieren schon aufgefallen, daß die Adressen, an denen die einzelnen Befehle liegen, ziemlich unregelmäßig durchnumeriert werden. Das liegt daran, daß die Befehle unterschiedlich viel Platz im Speicher benötigen. Die 6502-CPU kennt Befehle, die ein, zwei oder drei Bytes belegen. Diese Instruktionslänge ist abhängig von der Adressierungsart. So sind die Befehle mit implizierter Adressierung (Das sind die ohne Argument.) nur ein Byte lang, bei unmittelbarer Adressierung (gekennzeichnet durch ein Doppelkreuz) werden zwei und bei absoluter drei Bytes belegt.

Programme sind auch nur Daten

Der eigentliche Befehl steckt dabei immer im ersten Byte. In ihm ist auch die Instruktionslänge verschlüsselt. Die beiden Versionen des LDA-Befehles, die Sie bislang kennen, haben zum Beispiel auch unterschiedliche Instruktions-Bytes. Bei der Immediate-Adressierung ist es $A9 und bei absoluter Adressierung $AD. Dadurch erkennt der Prozessor die unterschiedliche Adressierungsart und damit auch die Instruktionslänge.

Wenn der Prozessor beginnt, ein Programm abzuarbeiten, liest er das erste Byte. Bei Bedarf werden dann noch ein oder zwei Bytes gelesen, der Befehl ausgeführt, und das Spiel wird mit dem ersten Byte des nächsten Befehls fortgeführt.

Normalerweise wird also ein Byte nach dem anderen gelesen und die entsprechende Aktion durchgeführt. Sie werden in dieser Folge aber noch Kommandos kennenlernen, mit denen man diese Reihenfolge beeinflussen kann. Eines kennen Sie schon, nämlich BRK. Trifft der Prozessor auf diesen Befehl, macht er an einer speziellen Adresse weiter. Diese Adresse ist innerhalb des ROMs. Das Programm, das dort steht, löscht normalerweise den Bildschirm, gibt das Wort READY aus und wartet auf eine Eingabe.

Aus dem bisher gesagten erkennt man (hoffentlich), daß ein Maschinenprogramm im Prinzip nichts anderes ist als eine Folge von Bytes, die hintereinander im Speicher liegen. Mit dem Ende eines Programmes wird aber nicht das Ende des Speichers erreicht. Wenn ein

Zum Programm

Die INPUT 64-Assembler-Schule setzt sich aus mehreren Teilen zusammen. Nach dem Laden sehen Sie ein Titelbild, von dem aus Sie mit einem beliebigen Tastendruck in das Hauptmenue gelangen.

Wenn Sie nun F1 druecken, gelangen Sie in ein Menue, das Ihnen verschiedene Themen zur Auswahl stellt. Die Erklärungen, die Sie jetzt abrufen können, sollten Sie parallel zum Beiheft lesen. Beide Medien ergänzen sich hier. Sie können die Erklärungen auch mit CTRL-b ausdrucken. Ins Hauptmenue gelangen Sie jederzeit mit der STOP-Taste zurück.

Mit F3 gelangen Sie aus dem Hauptmenue zu einer Auswahl verschiedener Beispielprogramme.

Programm also einfach endet, ohne mit einem BRK oder einem anderen geeigneten Befehl (Sie werden noch verschiedene kennenlernen) abgeschlossen zu werden, versucht der Prozessor, die folgenden Bytes auch als Programm zu interpretieren und auszuführen. Dabei entstehen die verrücktesten Effekte, meistens endet so etwas mit einem 'Absturz' des Rechners.

Innerhalb unseres Simulators kann nichts passieren, Sie erhalten eine entsprechende Fehlermeldung. Wenn Sie aber ein Programm 'im richtigen Leben' laufen lassen, das in Simulator mit der Meldung „Programmende" oder „Opcode nicht ausführbar" abbricht, sollten Sie sich über nichts wundern. Kaputtgehen kann der C64 dabei nicht, aber Sie werden wahrscheinlich einen Reset-Taster oder gar den Netzschalter betätigen müssen.

Genauso, wie man Bytes im Speicher entweder als Programm oder als Daten auffassen kann, gibt es für Datenbytes meistens verschiedene Interpretationsmöglichkeiten.

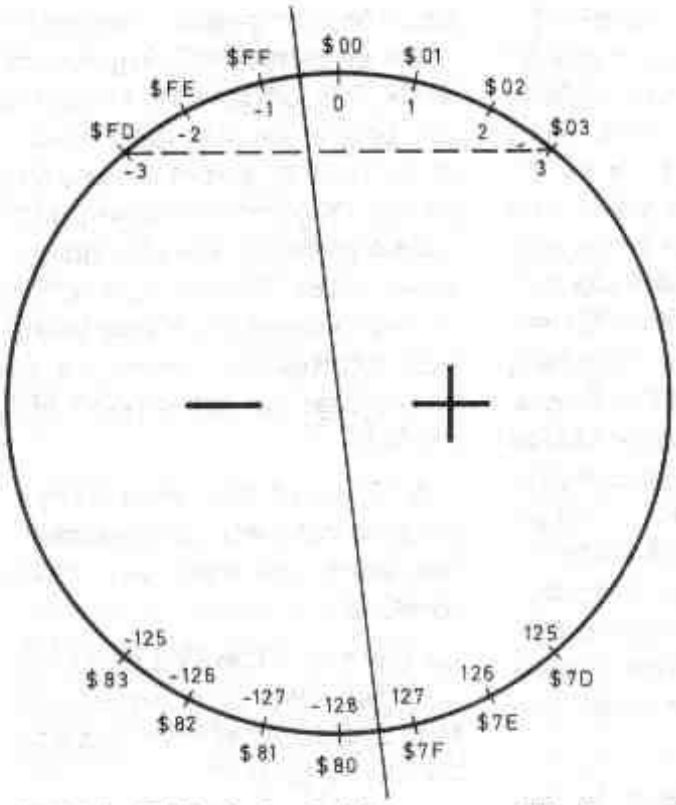


Bild 1: Im Zahlenkreis wird das Prinzip des Zweierkomplementes deutlich: Die komplementären Zahlen liegen einander jeweils gegenüber. Beim Überschreiten der Grenze am unteren Ende liegt ein Überlauf vor.

Sie können eines davon auswählen, das Sie sich dann im Editor anschauen oder auch verändern können. Wenn Sie an dieser Stelle eine Null eingeben, enthält der Editor das zuletzt bearbeitete Programm, beim ersten Aufruf ist der Textspeicher leer.

Wenn Sie ein Beispielprogramm bearbeitet haben und - mit der STOP-Taste - wieder ins Hauptmenue springen, können Sie Ihren Text auch auf einen Drucker ausgeben lassen oder auf einen eigenen Datenträger abspeichern. Abgespeicherte Programme können Sie direkt mit dem INPUT-Ass (Ausgabe 6/86) laden und weiterbearbeiten.

Vom Editor aus gelangen Sie mit F7 in einen integrierten Simulator. Hier können Sie unsere Programmbeispiele oder Ihre selbstentworfenen Programme ablaufen lassen und testen, ob sie sich erwartungsgemäß verhalten.

Ausführliche Hinweise zur Bedienung des Editors und des Simulators sind im Programm enthalten. Sie können Sie von dort aus jeweils mit der Funktionstaste F6 aufrufen. Es wird empfohlen, diese Seiten vor der Benutzung des Programmpakets einmal gründlich zu lesen. Besitzer eines Druckers können sie auch mit CTRL-b zu Papier bringen.

Die INPUT 64-Assemblerschule ist eine Serie, die in der Ausgabe 3/87 begonnen hat. Die einzelnen Lektionen bauen aufeinander auf. Wer noch keine Erfahrungen mit der Maschinensprache-Programmierung hat, tut gut daran, mit der ersten Folge anzufangen.

Weniger als nichts

In der ersten Folge haben wir unter anderem gelernt, wie Ein- und Zwei-Byte-Werte in Maschinensprache subtrahiert werden. Dabei diente die Carry-Flagge des Prozessor-Status-Registers als Anzeige für einen Übertrag in die nächsthöhere Stelle beziehungsweise für einen Fehler. Wenn bei der Subtraktion eine negative Zahl herauskam, sind wir davon ausgegangen, daß ein Fehler vorliegt. Mit Hilfe des sogenannten Zweierkomplementes ist es nun möglich, auch negative Ergebnisse sinnvoll zu interpretieren. Dabei werden alle Bytes mit gesetztem höchstwertigem Bit als negative Zahlen aufgefaßt. Das genaue Umrechnungsverfahren ist im Programm beschrieben.

Je nachdem, wie die Ergebnisse einer Rechnung weiterverarbeitet werden, kann man also die Zahlen $80 bis $FF einfach umrechnen und ihnen die Werte 128 bis 255 zuordnen oder mit Hilfe des Zweierkomplementes als die negativen Zahlen -128 bis -1 auffassen. Diese Tatsache wird durch den Zahlenkreis anschaulich verdeutlicht.

Bei letzterer Darstellungsweise kann es

natürlich auch zu Über- beziehungsweise Unterschreitungen des gültigen Zahlenbereiches kommen. Addiert man beispielsweise die Zahlen 73 und 58, so ist das Ergebnis größer als 127, das höchstwertige Bit ist gesetzt, und daher wäre das Resultat als negative Zahl zu interpretieren. Zum Glück stellt der Prozessor auch für diesen Fall eine Möglichkeit der Bereichsüberprüfung zur Verfügung. In dem obigen Beispiel wäre nach der Ausführung der Addition die Overflow-Flagge im Statusregister gesetzt. Dieses Bit – auch V-Flag genannt – wird automatisch bei jeder Addition und Subtraktion mitversorgt, ähnlich wie die Carry-Flagge. Sein Inhalt hat aber auf eventuell folgende ADC- oder SBC-Befehle keinen Einfluß.

Hier die Regeln, nach denen der Prozessor die V-Flagge setzt: Die CPU geht immer davon aus, daß sie es mit vorzeichenbehafteten Zahlen zu tun hat. Die V-Flagge wird gesetzt, wenn zu einer positiven Zahl eine positive Zahl addiert oder von ihr eine negative Zahl subtrahiert wird und dabei das Ergebnis größer als 127, also negativ, ist. Im negativen Bereich ist es ebenso: Negative Zahl plus negative Zahl oder negative Zahl minus positive Zahl und positives Ergebnis ergibt gesetztes Overflow-Flag.

Das hört sich zwar sehr kompliziert an, ist es aber eigentlich gar nicht, denn es geschieht völlig automatisch. Wenn man mit vorzeichenbehafteten Zahlen rechnet, sollte man nach einem ADC- oder SBC-Befehl die V-Flagge prüfen. Sie können sich einfach darauf verlassen, daß das Ergebnis stimmt, wenn sie nicht gesetzt ist. Wie man ein Flag des Status-Registers innerhalb eines Programmes prüft, dazu kommen wir gleich.

Statusfragen

Zunächst wollen wir einen ausführlichen Blick auf die einzelnen Bits des Prozessor-Status-Registers – auch kurz P-Register genannt – werfen. Es ist wie die meisten 6502-Register acht Bits breit. Jedoch kann man es nicht wie zum Beispiel den Akku direkt manipulieren. Vielmehr werden einzelne Bits bei der Programm-Ausführung automatisch beeinflußt. Wie wir schon gesehen haben, können einzelne Bits auch vom Programmierer direkt gesetzt oder zurückgesetzt werden wie die Carry-Flagge mit den Befehlen SEC und CLC.

Jedes Flag wird durch einen Buchstaben gekennzeichnet. Die Bezeichnungen lauten von links nach rechts NV-BDIZC

Die Bits 0 (C = Carry-Flag) und 6 (V, Overflow) hatten wir schon. Bit 5 hat keine Bedeutung und ist Hardware-bedingt immer gesetzt.

Mit den bisher bekannten Befehlen haben wir die Bits 1 und 7 auch schon beeinflußt, aufmerksame Beobachter haben es vielleicht beim Experimentieren bemerkt.

Bit 1 heißt Zero- oder kurz Z-Flagge. Der Prozessor setzt sie immer, wenn das Ergebnis eines Ladebefehles oder einer arithmetischen Operation gleich Null ist. Bei anderen Resultaten wird die Zero-Flag wieder gelöscht.

Bit 7, die N-Flagge, zeigt das Vorzeichen des Ergebnisses an. Sie übernimmt bei einem Ladebefehl oder einem ADC- oder SBC-Kommando das höchstwertige Bit des Ergebnisses. Sie ist also bei einem negativen Resultat gesetzt und bei einem positiven gelöscht. Daher auch ihr Name Negative-Flag.

Diese Flaggen werden auch von anderen Befehlen beeinflußt. Wenn diese an der Reihe sind, werden wir auf diese Nebenwirkungen eingehen.

Zukunftsmusik

Bit 3 des Statusregisters ist ein Prozessor-interner Schalter. Mit speziellen Befehlen kann der Programmierer dieses Flag setzen oder löschen und den Prozessor dadurch in den sogenannten Dezimal-Modus schalten. Die Auswirkungen dieses Schalters werden wir in der nächsten Folge ausführlich besprechen.

Mit den Bits 2 und 4 kann man externe Programm-Unterbrechungen (Interrupts) kontrollieren. Die I-Flagge dient dabei als Schalter und teilt dem Prozessor mit, ob solche Interrupts zugelassen sind. Mit der B-Flagge (Break-Flag) kann man feststellen, woher diese Unterbrechung kam. Sie wird immer gesetzt, wenn der Prozessor auf einen BRK-Befehl trifft. Dann springt der Rechner nämlich zu der gleichen Adresse wie bei einem Interrupt. Diese ist – der Prozessor erwartet es so – in den Adressen $FFFE und $FFFF des ROMs verzeichnet. Mehr zu diesen Flags in einer späteren Folge der Assembler-Schule.

Immer diese Entscheidungen

Jetzt wollen wir aber endlich wieder programmieren! Mit den ersten neuen Befehlen, die Sie kennenlernen sollen, lüften wir das Geheimnis, wie man einzelne Flags des Status-Registers prüfen kann. Das funktioniert bei den Bits Carry, Overflow, Zero und Negative. Das Zauberwort heißt Bedingter Sprung, auf gut Englisch Branch. Die Branch-Befehle testen das entsprechende Status-Bit und führen gebenenfalls einen Sprung aus. Ist die Bedingung nicht erfüllt, wird einfach beim nächsten Befehl

N	V	–	B	D	I	Z	C

Bild 2: Im Prozessor-Status-Register hat jedes Bit eine besondere Bedeutung.

Opcode	Bedeutung	Bedingung
BPL	Branch on result PLus	N-Flag = 0
BMI	Branch on result MInus	N-Flag = 1
BVC	Branch on oVerflow Clear	V-Flag = 0
BVS	Branch on oVerflow Set	V-Flag = 1
BCC	Branch on Carry Clear	C-Flag = 0
BCS	Branch on Carry Set	C-Flag = 1
BNE	Branch on result Not Equal	Z-Flag = 0
BEQ	Branch on result EQual	Z-Flag = 1

Tabelle 1: Mit bedingten Sprüngen trifft der Prozessor Entscheidungen.

weitergemacht. Alle Branch-Befehle des 6502 zeigt Tabelle 1.

Als Parameter verlangen diese Befehle natürlich noch das Sprungziel. In unserem Simulator und wenn Sie mit einem Assembler arbeiten, können Sie einfach die Adresse des Zieles oder noch besser ein Label, das an dieser Adresse steht, hinter den Branch-Befehl schreiben. Der Prozessor benutzt aber nicht diese Adresse sondern die Differenz zwischen dem nächsten Befehl und dem Sprungziel. Diese Umrechnung führt der Assembler für Sie durch.

Dieser berechnete Offset ist ein Ein-Byte-Wert in Zweierkomplement-Form. Bei einem Rücksprung ist er negativ, bei einem Sprung nach vorne positiv. Mit Branches kann man höchstens 128 Bytes rückwärts beziehungsweise 127 Bytes nach vorne springen. Diese Adressierungsart, die es ausschließlich bei den Verzweigungs-Befehlen gibt, heißt Relative Adressierung. Diese Befehle haben eine Instruktionslänge von zwei Bytes.

Fehlerfalle

Nach so viel Erklärungen sollte das erste Beispielprogramm für Sie keine Geheimnisse mehr bergen. Die ersten drei Befehle sind altbekannt. Danach kommt eine Programmverzweigung. Wenn bei der Addition alles glattgegangen ist, wird der Befehl bei $C00F, Label OKAY, angesprungen. Das Ergebnis der Addition wird dann in SUM2 gespeichert, und das Programm ist fertig.

Ist nach der Addition die V-Flagge gesetzt, wird das Ergebnis verworfen. Stattdessen wird $FF nach Flag gespeichert. Dadurch kann auch nach dem Programmende noch ein Fehler festgestellt werden, zur Not durch PEEK(49173).

Sie sollten in diesem Programm mit den Werten für SUM1 und SUM2 experimentieren und auch den ADC-Befehl mal durch SBC ersetzen. Beobachten Sie dabei auch, was mit den Flaggen Carry, Zero und Negative passiert.

XY aufgelöst

Das zweite Programm bringt eine Reihe neuer Befehle. Gleich der erste ist noch unbekannt. Aber keine Angst, so neu ist er auch wieder nicht.

LDX

heißt LoaD X-register. Er funktioniert fast wie LDA, nur daß eben nicht der Akku sondern das Index-X-Register geladen wird. Für das Index-Y-Register gibt es diesen Befehl auch, er heißt

LDY

Beide Befehle gibt es in der Immediate- und der Absolute-Version, beide beeinflussen – wie LDA – die Flaggen Negative und Zero.

Der nächste Befehl im Programm heißt

TXA

und ist die Abkürzung für Transfer X-register to Akku. Er gehört zu einer Vierergruppe von Befehlen, die Prozessor-intern den Datenverkehr zwischen dem Akku und den Index-Registern ermöglichen. Die anderen drei heißen

TYA (Transfer Y to Akku),

TAX (Transfer Akku to X) und

TAY (Transfer Akku to Y).r

Alle vier sind Ein-Byte-Befehle mit der Adressierungsart Implied, sie beeinflussen die N- und die Z-Flagge.

Den nächsten Befehl wollen wir erstmal übergehen und wenden uns dem Kürzel

INX

zu. Es bedeutet INcrement X-register. Auch dieser Befehl hat drei Geschwister. Sie heißen

INY (INcrement Y-register),

DEX (DEcrement X-register) und

DEY (DEcrement Y-register).

Diese vier Befehle sind unter anderem dafür verantwortlich, daß man die Index-Register X und Y so gerne benutzt. Sie ermöglichen es es nämlich, mit einem schnellen und kurzen Ein-Byte-Befehl den Inhalt des entsprechenden Registers um Eins zu erhöhen (increment) oder zu vermindern (decrement). Damit eignen sich die Index-Register hervorragend als Zähler für Programmschleifen. Für den Akku gibt es solche Befehle (vielleicht INA oder DEA) leider nicht.

Diese vier Befehle setzen je nach Ergebnis die Zero- und die Negative-Flag. Alle vier gibt es nur als impliziert adressierte Ein-Byte-Befehle.

Programmieren mit System

Der letzte unbekannte Befehl in diesem Programm gehört eigentlich noch gar

nicht in diese Lektion. Seine genaue Funktionsweise kommt in der nächsten Folge. Hier nur soviel:

JSR

heißt Jump to SubRoutine, zu Deutsch „Springe in ein Unterprogramm". Er funktioniert ähnlich dem BASIC-Befehl GOSUB. Nach der Ausführung der Unterroutine wird das Programm beim nächsten Befehl fortgesetzt.

Das Kürzel PRCH ist ein innerhalb des Simulators vordefiniertes Label und soll an PRint CHaracter erinnern. Das Unterprogramm, zu dem diese Adresse gehört, gibt auf dem Bildschirm das Zeichen aus, dessen ASCII-Code im Akku des Prozessors steht. Im Betriebssystem-ROM des C64 gibt es eine solche Routine an der Adresse $FFD2. Sie ist normalerweise unter dem Namen BSOUT bekannt.

Rücksprünge ergeben Schleifen

Sehen wir uns das Programm nun in Aktion an. Falls Sie es noch nicht getan haben, laden Sie es in den Editor und drücken F7, um es zu assemblieren. Der Befehl LDX #$20 lädt den ASCII-Code des Leerzeichens — das kleinste druckbare Zeichen — ins X-Register. Der nächste Befehl kopiert diesen Wert in den Akku, wo die Routine PRCH ihn erwartet. Nach der Ausgabe des Zeichens (Leerzeichen ist nicht zu sehen) wird der Inhalt des X-Registers um Eins erhöht. $21 ist kleiner als 127, also positiv. Darum ist die N-Flagge gleich Null, und der Rücksprung wird ausgeführt.

Jetzt wird die Schleife erneut durchlaufen und ein Ausrufezeichen ausgegeben. Wenn Sie es nicht sehen, liegt das wahrscheinlich daran, daß Sie im unteren Drittel des Bildschirmes den Monitor eingeschaltet haben. Drücken Sie die HOME-Taste, und Sie sehen an der selben Stelle vier inverse Leerzeilen. Sie stellen in unserem Simulator den Bildschirm dar, auf den die Routine PRCH zugreift.

Sie können nun die Pfeil-aufwärts-Taste drücken, um die Geschwindigkeit zu erhöhen. Nacheinander sollten auf dem 'Bildschirm' die Zeichen bis CHR$(127) gedruckt werden.

Vergleichen Sie bitte

Der letzte neue Befehl dieser Lektion taucht im dritten Beispielprogramm auf und heißt

CMP

(CoMPare to accumulator — vergleiche mit Akku). Er führt eine Subtraktion aus wie der Befehl SBC mit vorher gesetzter Carry-Flagge. Das Ergebnis dieser Subtraktion wird jedoch nicht in den Akku übernommen. Der Befehl CMP dient lediglich dazu, die Flaggen N, Z und C im Status-Register entsprechend zu setzen.

Nach der Ausführung eines CMP-Befehles ist also die Z-Flagge gesetzt, wenn das Argument und der Inhalt des Akkumulators gleich waren. Wenn die Carry-Flagge gesetzt ist, bedeutet das, daß das Argument größer oder gleich dem Akku-Inhalt ist, gelöschte Carry heißt kleiner.

Der JSR-Befehl tritt in unserem dritten Beispiel mit der Adresse GETC auf. Auch dieses ist ein vordefiniertes Label. Die dazugehörige Betriebssystem-Routine verhält sich ähnlich wie der BASIC-Befehl GET: Bei der Rückkehr aus diesem Unterprogramm enthält der Akku den ASCII-Code der zuletzt gedrückten Taste. Wurde keine Taste gedrückt, so ist die Z-Flagge gesetzt, und im Akku steht eine Null.

Mit Filter

Das Programm fragt die Tastatur ab. Es bricht ab, wenn die RETURN-Taste (ASCII 13) gedrückt wird. Bei anderen Tasten wird überprüft, ob es sich um eine Ziffer handelte. Der Befehl CMP #'0 stellt keine neue Adressierungsart dar, sondern nutzt die Fähigkeit des Assemblers aus, Zeichen in deren ASCII-Wert umzurechnen. Bei der Programmausführung wird dieser Befehl zu CMP #$30, denn $30 (48) ist der ASCII-Code des Zeichens Null.

Die ASCII-Codes in Ihrem C64-Handbuch auf Seite 135ff haben übrigens auch in Maschinensprache Gültigkeit. Der Doppelpunkt ist demnach das nächsthöhere Zeichen nach der 9. Die Befehlsfolge CMP und BCS vergleicht ja auf 'größer oder gleich'. Würde an dieser Stelle CMP #'9 stehen, so würde das Programm die 9 abweisen.

Wenn das eingegebene Zeichen kleiner als 0 oder größer als 9 ist, springt das Programm wieder zur Eingabeschleife. Ziffern werden auf dem Bildschirm ausgegeben.

Sie sollten versuchen, dieses doch schon recht komplizierte Programm in allen Einzelheiten zu verstehen. Es zeigt, wie vielfältig die Branch-Befehle eingesetzt werden können. Dieses Programm dient auch als Grundlage zur Hausaufgabe (siehe Programm auf Ihrem Datenträger).

Wenn Sie irgendetwas nicht verstanden oder einen Fehler entdeckt haben, oder wenn Sie Verbesserungen zu dieser Serie vorschlagen möchten, rufen Sie bitte nicht in der Redaktion an, sondern schreiben Sie uns unter dem Stichwort „Assembler-Schule". Dann erreichen Sie garantiert den zuständigen Mitarbeiter.

In der nächsten Lektion lernen Sie, wie Sie selbst Unterprogramme schreiben. Außerdem gibt es wieder Beispielprogramme zum Thema Arithmetik. HS

Literatur

Christian Persson,
6502/ 65C02 Maschinensprache,
Verlag Heinz Heise GmbH, Hannover,1983

Rodnay Zaks,
Programmierung des 6502,
Sybex-Verlag GmbH, Düsseldorf, 1981

In die Tiefe

INPUT 64-Assemblerschule, Teil 3

In der letzten Folge wurde ja schon der JSR-Befehl vorgestellt. Wir haben gesagt, daß die Abkürzung von 'Jump to SubRoutine' (Springe in ein Unterprogramm) kommt. Hin und wieder liest man auch 'Jump Saving Returnadress' (Springe und rette Rückkehradresse). Diese Interpretation werden Sie verstehen, wenn Sie die genaue Funktionsweise kennengelernt haben. Allerdings müssen wir dazu etwas weiter ausholen.

Der Befehl JSR benutzt den Prozessor-Stack. 'Stack' ist mal wieder ein englisches Wort, übersetzt heißt es Stapel. Dabei handelt es sich um einen besonderen, für diesen Zweck reservierten Speicherbereich. Er liegt bei 6502-Computern an den Adressen $100 bis $1FF, also in der Speicherseite 1.

Man kann sich den Stack anschaulich wie einen Stapel aus Notizzetteln vorstellen: Sie können auf einen solchen Stapel Zettel oben draufliegen oder von oben jeweils einen wegnehmen. Lesen kann man immer nur den obersten.

In dieser Lektion unseres Maschinensprache-Lehrgangs werden wir uns im doppelten Sinne in neue Tiefen wagen. Zum einen werden Sie den Kellerspeicher kennenlernen. Zum anderen steigen wir von der Ebene der Bytes noch eine Stufe tiefer und schauen uns Befehle an, mit denen einzelne Bits manipuliert werden können. Wenn Sie durch die Beschäftigung mit der Maschinensprache bereits sechzehn Finger haben, werden Sie es vielleicht auch als Abstieg empfinden, daß wir gegen Ende dieses Kapitels wieder im Dezimalsystem rechnen.

Tiefstapler

Der Prozessor-Stack beginnt an der Adresse $1FF und 'wächst' abwärts. Die CPU besitzt zur Verwaltung des Stapels ein eigenes Register, den Stackpointer (Stapelzeiger). In unserem Simulator wird sein Inhalt in der Spalte unter 'SP' angezeigt. Der Stackpointer zeigt immer auf die nächste freie Speicherstelle im Stack. Diesen Mechanismus zeigt Bild 1: Die ersten vier Einträge im Stapel ($1FF bis $1FC) enthalten bereits Informationen. Legt ein Programm nun etwas auf dem Stack ab, so wird die Speicherstelle $1FB beschrieben und gleichzeitig der Stackpointer um Eins vermindert. Beim Lesen aus dem Stack erhöht der Prozessor den Inhalt des Stackpointers um Eins und liest die Speicherstelle $1FC.

Wenn der Prozessor nun auf einen JSR-Befehl trifft, so schreibt er den augenblicklichen Inhalt des Programmzählers auf den Stack, zuerst das höherwertige und dann das niederwertige Byte. Auf diese Art 'merkt' er sich die Adresse des Unterprogrammaufrufes. Dann springt er zu der im Befehl angegebenen Adresse. (Aus Prozessor-internen Gründen wird übrigens die Adresse des dritten Bytes des JSR-Befehles abgespeichert.)

Am Ende eines jeden Unterprogrammes steht der Befehl

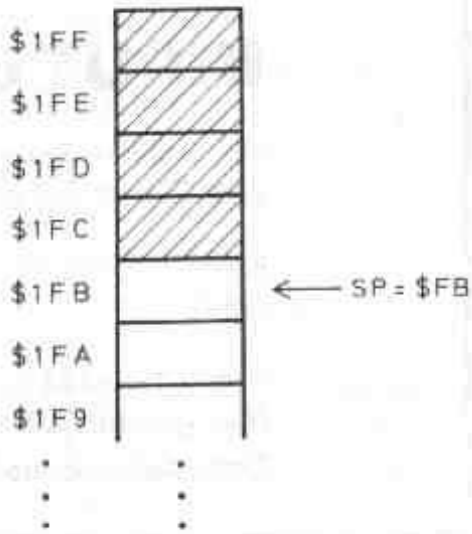
RTS

(ReTurn from Subroutine, zu deutsch Rückkehr aus Unterprogramm). Er wird folgendermaßen abgearbeitet: Die CPU holt sich die oberen beiden Bytes vom Stack und lädt sie in den Programmzähler. Der wird dann um Eins erhöht, und an dieser Adresse setzt der Prozessor seine Arbeit fort. An dieser Stelle steht ja genau der nächste Befehl nach dem JSR-Kommando.

Stapellauf

Auf diese Weise kann sich der Prozessor bis zu 128 ineinander verschachtelte Unterprogrammaufrufe merken (Je-

Bild 1: Der Prozessor-Stack wächst abwärts. Die schraffierten Kästchen stellen bereits belegte Speicherstellen dar.



der belegt zwei Bytes, der Stack kann 256 Bytes aufnehmen.). Das erste Beispielprogramm auf Ihrem Datenträger verdeutlicht diesen Mechanismus.

Es beginnt mit einem Sprung in das Unterprogramm INPT, das die Aufgabe hat, die Tastatur abzufragen, die Anzahl der Tastendrücke zu zählen und bei Eingabe der RETURN-Taste abzubrechen. Dazu benutzt es die Routine WAIT. Diese aktiviert in einer Schleife die Betriebssystem-Routine GETC so lange, bis eine Taste gedrückt wird. WAIT gibt den Wert der betätigten Taste im Akku zurück. INPT prüft dann, ob es die RETURN-Taste war. In diesem Falle bricht sie ab und gibt die Anzahl der gedrückten Tasten im X-Register an das aufrufende Programm zurück. Anderenfalls wird das X-Register inkrementiert und die Tastatur erneut abgefragt. Im Hauptprogramm wird nach Beendigung des Unterprogramms INPT die Anzahl der Tasten in der Speicherstelle ZAHL gespeichert und vor dem Programmende noch ein erneuter Tastendruck abgewartet.

Wenn Sie das Programm starten, achten Sie auf den jeweiligen Inhalt des Stackpointers. Mit der Minus-Taste können Sie sich auch den Stack ansehen. Interessant sind hier die Adressen $1F8 bis $1FF. Wie Sie sehen, wird bei der Ausführung des RTS-Befehles im Stack selber nichts geändert. Durch die Inkrementierung des Stackpointers ist die Rückkehradresse jedoch aus der Sicht des Prozessors aus dem Stack entfernt.

Bestimmt haben Sie die Bedeutung des zweiten Befehles im Beispielprogramm schon erraten, er sei hier aber der Vollständigkeit halber noch erklärt.

STX

heißt STore X-register und speichert den Inhalt des Index-X-Registers an der angegebenen Speicheradresse ab. Wie Sie völlig richtig vermuten, gibt es diesen Befehl auch für das Y-Register, er heißt dann

STY

Schiebung

Wo wir schon mal dabei sind, neue Befehle zu lernen, können wir eigentlich auch gleich damit weitermachen. Die nächsten vier Instruktionen bilden die Gruppe der Schiebe- und Rotationsbefehle. Ihre Funktionsweise ist in Bild 2 dargestellt. Links sehen Sie die beiden Schiebebefehle. Sie heißen

ASL (Arithmetic Shift Left)
und
LSR (Logical Shift Right).

Sie bewirken eine Verschiebung des angesprochenen Bytes um eine Bitstelle nach links (ASL) beziehungsweise nach rechts (LSR). Das dabei freiwerdende Bit wird mit einer Null aufgefüllt, das herausgeschobene Bit landet in der Carry-Flagge. Neben der Carry werden je nach Ergebnis noch die Zero- und die Negativ-Flagge beeinflußt.

Mit den Schiebebefehlen kann man — je nach Adressierungsart — entweder den Akku-Inhalt verändern oder auf eine Speicherstelle zugreifen. Ohne Argument (Adressierungsart Implied) fühlt sich der Akku angesprochen, ansonsten die angegebene Adresse. (Allerdings verlangen einige Assembler die Schreibweise 'ASL A', wenn die Implied-Version gemeint ist.)

Diese Befehle werden sehr oft benötigt, wenn irgendwelche Bytes bitweise verarbeitet werden sollen. Außerdem dienen sie zur Multiplikation und Division. Wenn man im Dezimalsystem eine Zahl um eine Stelle nach links verschiebt, ergibt das eine Multiplikation mit Zehn. Genauso entspricht die Verschiebung einer Binärzahl um ein Bit nach links einer Multiplikation mit Zwei. Analog ergibt das Verschieben nach rechts eine Division.

Bitkarussell

Die beiden anderen Operationen dieser Vierergruppe sind die sogenannten Rotationsbefehle. Sie sind den Schiebebefehlen sehr ähnlich. Die Abkürzungen für die Rotationsbefehle sind

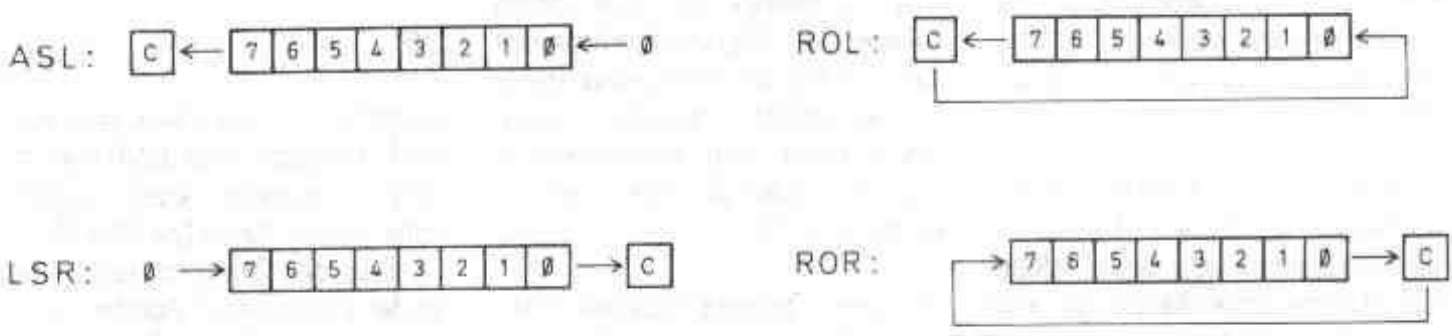


Bild 2: Die Schiebe- und Rotationsbefehle benutzen die Carry-Flagge als achtes Bit.

ROL (ROtate Left)
und
ROR (ROtate Right).

Auch bei ihnen wird das jeweilige Byte um ein Bit nach links (ROL) oder nach rechts (ROR) verschoben, wobei das überschüssige Bit in die Carry gelangt. Am anderen Ende wird jedoch nicht eine Null nachgeschoben sondern der Inhalt, den die Carry vor der Ausführung des Befehles hat.

Für die Rotationsbefehle gilt in Bezug auf die Beeinflussung der anderen Status-Flaggen und die Adressierungsarten das gleiche wie bei den Schiebebefehlen.

Diese Operationen werden benötigt, wenn der Inhalt der Carry-Flagge von Bedeutung ist. Zum Beispiel kann man eine Zwei-Byte-Zahl mit der Befehlsfolge

ASL Low-Byte

ROL High-Byte

verdoppeln. Das höchste Bit des Low-Bytes landet dabei in Bit 0 des High-Bytes.

Logisch!

Die nächste Gruppe von Befehlen, die Sie kennenlernen sollen, stellen drei verschiedene Operationen zur Verfügung. An ihnen ist — ähnlich wie bei den Befehlen ADC und SBC — der Akku und ein anderes Byte beteiligt. Alle drei kennen dieselben Adressierungsarten wie ADC und SBC, und sie beeinflussen die Negativ- und die Zero-Flagge. Es handelt sich um die logischen Verknüpfungen von Binärzahlen.

Der 6502-Prozessor kennt Maschinenbefehle für die drei Logik-Funktionen Und, Oder und Exklusiv-Oder. Die Wertetabellen der drei Verknüpfungen sind in Tabelle 1 enthalten.

A	B	A AND B	A OR B	A EXOR B
0	0	0	0	0
0	1	0	1	1
1	0	0	1	1
1	1	1	1	0

Tabelle 1: Die Funktionsweise der logischen Operationen erkennt man aus ihren Wahrheitstafeln.

Der zur Und-Verknüpfung gehörende Maschinensprache Befehl heißt

AND (AND with akku)

Mit ihm werden der Akku und das Argument bitweise gemäß der abgebildeten Wertetabelle verknüpft. Das Ergebnis steht danach im Akku.

Mit diesem Befehl lassen sich gezielt Bits im Akku löschen. Alle Bits, die im Argument gleich Null sind, sind es auch im Ergebnis. Ein im Argument gesetztes Bit beeinflußt das entsprechende Akku-Bit nicht. Beispielsweise löscht der Befehl 'AND #$0F' das obere Nibble im Akku. Das niederwertige Nibble enthält nach der Ausführung immer noch seinen alten Wert. Diesen Vorgang nennt man Maskieren, das Byte $0F stellt eine Bit-Maske dar.

Mit dem Befehl

ORA (OR with Akku)

wird eine bitweise Oder-Verknüpfung zwischen dem Akku und dem Argument durchgeführt, dessen Ergebnis wieder im Akku steht. Mit ihm werden einzelne Bits im Akku gesetzt. Alle Eins-Bits im Argument werden als solche in den Akku übernommen.

Um eine bitweise Exklusiv-Oder-Verknüpfung zwischen dem Akku und einem Argument durchzuführen, benutzt man den Befehl

EOR (Exclusive OR with akku)

Auch bei ihm nimmt der Akku das Ergebnis auf. Alle Akku-Bits, die im Argument gesetzt sind, werden durch diesen Befehl invertiert. Mit 'EOR #$FF' kann man so auf einfache Art und Weise das Einerkomplement der im Akku stehenden Zahl berechnen lassen.

Neben dem gezielten Manipulieren einzelner Bits im Akku werden die logischen Verknüpfungen auch zum Testen von Zahlen verwendet. So ist nach einem EOR-Befehl die Z-Flagge genau dann gesetzt, wenn Akku-Inhalt und Argument gleich waren. Im Gegensatz zum SBC-Befehl bleiben die V-Flagge und die Carry jedoch erhalten.

Um die Wirkungsweise dieser drei Befehle zu verstehen, sollten Sie sie mit dem Simulator ausgiebig ausprobieren. Erinnern Sie sich dazu an Ihr allererstes Maschinensprache-Programm zurück.

Begib Dich direkt dorthin

Nach so viel Theorie wollen wir uns wieder mal einem Programm zuwenden. Das zweite Beispiel auf Ihrem Datenträger enthält eine Routine, mit der ein Byte in hexadezimaler Darstellung auf dem Bildschirm ausgegeben werden kann.

Warum das Programm mit dem Befehl

JMP

beginnt, steht einige Zeilen tiefer. Aber daß er ausgeschrieben JuMP heißt und 'springe' bedeutet, sollen Sie jetzt schon wissen. Dieser Drei-Byte-Befehl veranlaßt den Prozessor, seine Arbeit an der angegebenen Adresse fortzusetzen, und zwar ohne Rücksicht auf

den Inhalt des Status-Registers. Ein weiterer Unterschied zu den Branch-Befehlen ist, daß man mit JMP beliebige Entfernungen innerhalb des Speichers überbrücken kann. Die Zieladresse steht explizit im Befehl und nicht als Differenz zum augenblicklichen Stand des Programmzählers.

Sichtbarer Erfolg

In der nächsten Programmzeile wird ein Label eingeführt, unter dem unsere Routine das auszugebende Byte finden soll.

Die folgende Zeile ist das Sprungziel des JMP-Befehls und der Anfang des eigentlichen Programmes. Die ersten beiden Befehle sorgen dafür, daß ein Dollarzeichen als Kennung für 'Hexadezimal' ausgegeben wird.

Das auszugebende Byte wird alsdann in den Akku geladen und viermal nach rechts geschoben. Dadurch gelangt der Inhalt des oberen Nibbles — das ja zuerst auf dem Bildschirm erscheinen soll — in die unteren vier Bits des Akkus, und das obere Nibble wird gleich Null.

So wird es auch von der Routine PNIB erwartet, die dazu dient, eine Zahl zwischen $00 und $0F auszugeben. Nach ihrer Beendigung lädt das Programm den Inhalt von WERT erneut in den Akku und maskiert mit dem Befehl 'AND #$0F' das untere Nibble aus. So kann es ebenfalls mittels PNIB ausgegeben werden. Zu dem folgenden RTS kommen wir noch.

PNIB soll eine Hex-Ziffer ausgeben. Aus einer ASCII-Tabelle entnehmen wir: Die Ziffern 0 bis 9 haben die Codes $30 bis $39, zu den Buchstaben A bis F gehören die ASCII-Werte $41 bis $46.

Die Routine PNIB arbeitet nun folgendermaßen: Wie bereits gesagt, erwartet sie im Akku eine Zahl mit gelöschtem High-Nibble. Durch den ORA-Befehl werden die unteren vier Bits nicht angetastet (Im Argument sind sie gleich Null.), und das höherwertige Nibble erhält eine Drei. Für die Ziffern 0 bis 9 enthält der Akku also schon den richtigen Wert zur Übergabe an die Betriebssystem-Routine PRCH. Das wird durch die nächsten beiden Befehle überprüft. Sie bewirken einen Sprung zum Label OKAY, wenn der Akku eine ASCII-Ziffer enthält.

Den Befehl „CMP #'9+1" wollen wir etwas genauer unter die Lupe nehmen: Der Assembler erkennt beim Übersetzen an dem Apostroph, daß ein ASCII-Zeichen folgt und setzt dafür den entsprechenden Wert ein. Die Anweisung „+1" läßt ihn noch Eins addieren. Im Simulator liest sich der Befehl somit als „CMP #$3A", also Vergleich mit dem der 9 folgenden Zeichen. Und so soll es auch sein, weil die CMP-BCC-Sequenz auf 'kleiner' und nicht auf 'kleiner oder gleich' prüft.

Wird der Sprung nicht ausgeführt, so enthält der Akku mindestens $3A. Zu $41, dem Wert für ein A, fehlen also noch 7. Da beim Erreichen des ADC-Befehls die Carry in jedem Falle gesetzt ist, kann man sich sparen, sie zu löschen. Man gibt im Argument einfach einen weniger an. So erklärt sich der Befehl „ADC #6".

Das Folgende ist wieder simpel: Mit „JSR PRCH" wird das Zeichen ausgegeben, und der RTS-Befehl führt in das aufrufende Programm zurück.

Von BASIC nach Maschine

Das besprochene Programm eignet sich sehr gut als kleines Hilfsprogramm, das man auch von BASIC aus aufrufen kann. Dazu überspielen Sie es aus dem Hauptmenue der Assemblerschule auf einen eigenen Datenträger. Dann schalten Sie den Rechner kurz aus und wieder ein, laden den INPUT-Ass (Den Assembler aus INPUT 64, Ausgabe 6/86) und mit ihm das abgespeicherte Beispielprogramm. Assemblieren Sie es entweder in den Speicher oder, wenn Sie es für später lauffähig aufheben wollen, auf einen Datenträger. Dann können Sie es mit LOAD"name",8,1 einfach wieder laden.

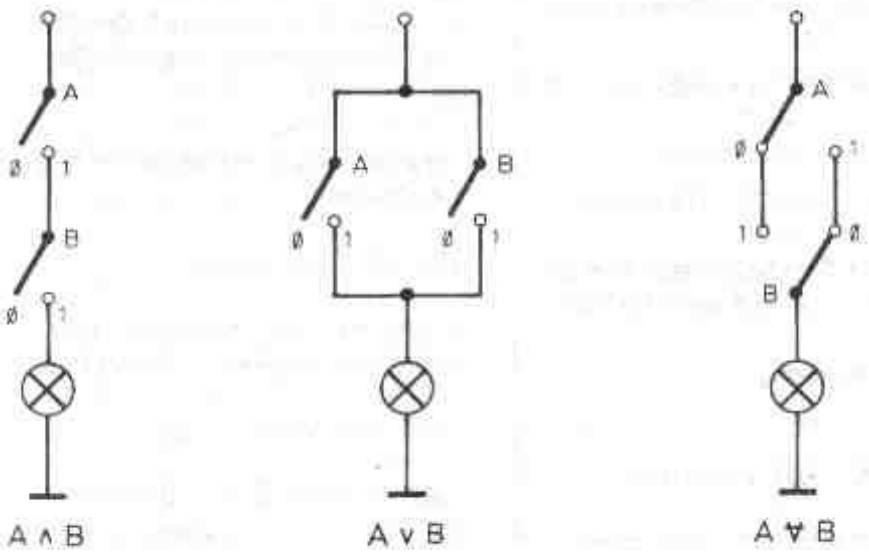


Bild 3: Die logischen Verknüpfungen AND, OR und EXOR lassen sich auch schaltungstechnisch darstellen.

Gestartet wird das assemblierte Programm mit SYS 49152 (49152 ist gleich $C000, der Startadresse). Vorher können Sie mit POKE 49155,zahl den auszugebenden Wert festlegen.

Nun zu dem oben angekündigten tieferen Sinn des JMP-Befehles am Anfang des Programmes: Bislang haben wir Zahlen immer hinter einem Programm aufgehoben. Solange man nur in Assembler programmiert, ist das auch in Ordnung. Bei einem Programm, das man aus BASIC heraus aufrufen will und das Werte übergeben bekommt, ist die hier vorgestellte Reihenfolge jedoch sinnvoller. Wenn Sie nämlich Änderungen an dem Programm vornehmen, etwa um hinter dem Byte noch ein RETURN auszugeben (Das sollten Sie übrigens mal probieren!), ändert sich automatisch die Programmlänge, und Sie müßten sich eine andere POKE-Adresse für die Wertübergabe merken.

. . . und wieder zurück

Der erste RTS-Befehl (der an der Adresse $C01B) bewirkt eine Rückkehr nach BASIC. Der BASIC-Interpreter legt nämlich bei der Ausführung des SYS-Befehles automatisch eine Rückkehr-Adresse auf dem Stack ab. Dadurch ist es möglich, auch aus BASIC-Programmen heraus eine Maschinensprache-Routine aufzurufen und anschließend mit dem folgenden BASIC-Befehl weiterzumachen.

Sie können in den bisherigen Beispielprogrammen den abschließenden BRK-Befehl auch durch ein RTS ersetzen, wenn Sie sie im BASIC-Direktmodus ausprobieren wollen. Dadurch vermeiden Sie, daß der Bildschirm nach der Abarbeitung gelöscht wird.

Innerhalb des Kurses liegt übrigens beim Start des Simulators immer die Startadresse des Editors auf dem Stack. Diese können Sie auch unter dem vordefinierten Label EXIT erreichen.

Zehn statt sechzehn

Zum Schluß wollen wir uns noch — wie in der letzten Folge angekündigt — die Wirkung der D-Flagge ansehen. Wenn sie gesetzt ist, arbeitet der Prozessor im sogenannten Dezimal-Modus. Für die Additions- und Subtraktionsbefehle werden dann Zahlen im BCD-Format verwendet. BCD heißt 'Binary Coded Decimal', also binär kodierte Dezimalziffer.

Tabelle 2: Der besseren Lesbarkeit und Genauigkeit der BCD-Darstellung fallen sechs Bit-Kombinationen zum Opfer.

Binär	BCD
%0000	0
%0001	1
%0010	2
%0011	3
%0100	4
%0101	5
%0110	6
%0111	7
%1000	8
%1001	9
%1010	ungültig
%1011	ungültig
%1100	ungültig
%1101	ungültig
%1110	ungültig
%1111	ungültig

Normalerweise kann man mit einem Nibble sechzehn verschiedene Zahlen darstellen. Im BCD-Code verwendet man nur zehn davon (Siehe Tabelle 2), also jeweils ein Nibble für eine Dezimalziffer.

Die gesetzte D-Flagge im Status-Register bewirkt nun, daß das Ergebnis einer Addition oder einer Subtraktion automatisch im BCD-Code dargestellt wird. Ein Überlauf in das nächsthöhere Nibble entsteht nicht erst beim Überschreiten von 15, sondern bereits wenn das Resultat größer als neun wird. Anschauliche Beispiele dazu finden Sie in den Erklärungen auf Ihrem Datenträger.

Der Befehl, mit dem man die D-Flagge setzt, heißt

SED (SEt Decimal-flag)

In den 'normalen' Rechenmodus können Sie den Prozessor mit dem Befehl

CLD (CLear Decimal-flag)

zurückschalten. Diesen Befehl sollten Sie auch zu Anfang eines jeden Pro-

Zum Programm

Die INPUT 64-Assembler-Schule setzt sich aus mehreren Teilen zusammen. Nach dem Laden sehen Sie ein Titelbild, von dem aus Sie mit einem beliebigen Tastendruck in das Hauptmenü gelangen.

Wenn Sie nun F1 drücken, gelangen Sie in ein Menü, das Ihnen verschiedene Themen zur Auswahl stellt. Die Erklärungen, die Sie jetzt abrufen können, sollten Sie parallel zum Beiheft lesen. Beide Medien ergänzen sich hier. Sie können die Erklärungen auch mit CTRL-b ausdrucken. Ins Hauptmenü gelangen Sie jederzeit mit der STOP-Taste zurück.

Mit F3 gelangen Sie aus dem Hauptmenü zu einer Auswahl verschiedener Beispielprogramme. Sie können eines davon auswählen, das Sie sich dann im Editor anschauen oder auch verändern können. Wenn Sie an dieser Stelle eine Null eingeben, enthält der Editor das zuletzt bearbeitete Programm, beim ersten Aufruf ist der Textspeicher leer.

Wenn Sie ein Beispielprogramm bearbeitet haben und - mit der STOP-Taste - wieder ins Hauptmenü springen, können Sie Ihren Text auch auf einen Drucker ausgeben lassen oder auf einen eigenen Datenträger abspeichern. Abgespeicherte Programme können Sie direkt mit dem INPUT-Ass (Ausgabe 6/86) laden und weiterbearbeiten.

Vom Editor aus gelangen Sie mit F7 in einen integrierten Simulator. Hier können Sie unsere Programmbeispiele oder Ihre selbstentworfenen Programme ablaufen lassen und testen, ob sie sich erwartungsgemäß verhalten.

Ausführliche Hinweise zur Bedienung des Editors und des Simulators sind im Programm enthalten. Sie können Sie von dort aus jeweils mit der Funktionstaste F6 aufrufen. Es wird empfohlen, diese Seiten vor der Benutzung des Programmpakets einmal gründlich zu lesen. Besitzer eines Druckers können sie auch mit CTRL-b zu Papier bringen.

Die INPUT 64-Assemblerschule ist eine Serie, die in der Ausgabe 3/87 begonnen hat. Die einzelnen Lektionen bauen aufeinander auf. Wer noch keine Erfahrungen mit der Maschinensprache-Programmierung hat, tut gut daran, mit der ersten Folge anzufangen.

grammes ausführen lassen, wenn unklar ist, in welchem Zustand sich der Prozessor beim Programmstart befindet.

Verwandlung

Das dritte Beispielprogramm in dieser Folge benutzt den Dezimal-Modus der CPU zur Umrechnung einer Zwei-Byte-Hexadezimalzahl in eine fünfstellige BCD-Zahl. Das Programm beginnt wieder mit einem Sprung, der die verwendeten Datenspeicher überbrückt.

Das eigentliche Programm beginnt mit dem Löschen des Ergebnis-Puffers. Dann wird das Index-Y-Register als Zähler für sechzehn Schleifendurchläufe — für jedes Bit einen — initialisiert und die Dezimal-Flagge gesetzt.

Die ersten beiden Befehle innerhalb der Schleife bewirken eine Verdoppelung der umzuwandelnden Zahl und eine Übertragung des höchstwertigen Bits in die Carry-Flagge.

Die folgenden neun Befehle bewirken beim ersten Schleifendurchlauf noch nicht viel. Jedoch handelt es sich hierbei um die Verdoppelung des Inhaltes des Ergebnisspeichers im BCD-Format mit gleichzeitiger Addition des Überlaufs aus ARGU. Dadurch, daß diese Schleife sechzehnmal durchlaufen wird, wird jedes Bit aus ARGU stellenrichtig zu ERGB addiert.

Nach dem letzten Schleifendurchlauf löscht das Programm die D-Flagge wieder und kehrt zum Aufrufpunkt zurück. Dort könnte beispielsweise eine Routine folgen, die den Inhalt von ERGB als fünfstellig formatierte Dezimalzahl auf dem Bildschirm ausgibt.

Diese Routine sollten Sie übrigens mit dem in dieser Folge Gelernten erstellen können. Das wäre dann auch die Hausaufgabe. Dazu ist zwar eine ganze Menge Tipparbeit nötig, aber immerhin entwickeln Sie auf diese Weise ein Programm, das — ähnlich wie das zweite Beispiel — einen praktischen Nutzen hat. Wie gewohnt werden wir Ihnen in der nächsten Folge eine Musterlösung vorstellen.

Außerdem sollten Sie auch im Juni wieder dabeisein, wenn Sie wissen wollen, warum die Indexregister Indexregister heißen und wie man mit Maschinensprache Ruck-Zuck Riesen-Speicherbereiche verschieben kann. Hajo Schulz

Viele Wege führen ins RAM

INPUT 64-Assembler-Schule, Teil 4

Sie erinnern sich bestimmt an die vier bereits vorgestellten Adressierungsarten: Die meisten Befehle arbeiten „immediate" und „absolute". Einige Befehle brauchen keine Parameter und sind „implied" adressiert, die Branch-Befehle benutzen ausschließlich die relative Adressierung.

Die 6502-CPU kennt aber insgesamt elf Adressierungsarten. Mit den bisher unbekannten werden Sie in der Lage sein, Programme zu schreiben, die auf Parameter und Adressen zugreifen, die nicht fest im Programm stehen, sondern erst während des Programmlaufes berechnet werden und sich ändern können. Die Adressierungsart, die wir zuerst betrachten wollen, stellt diese Möglichkeiten zwar nicht zur Verfügung, ermöglicht aber schnellere und kürzere Programme als bisher gewohnt.

Ging es in der letzten Folge der Assembler-Schule noch darum, einzelne Bytes in ihre Bestandteile zu zerlegen, so werden wir uns in dieser Lektion damit befassen, möglichst viele Bytes mit einem Befehl in den Griff zu bekommen. Wir zeigen ihnen, wie mit neuen Adressierungsarten die bekannten Befehle besser und flexibler einzusetzen sind.

Seite Null

Wie bereits in einer früheren Folge der Assembler-Schule erwähnt, ist der Speicher eines jeden 6502-Rechners in 256 Seiten zu je 256 Bytes eingeteilt. In der letzten Lektion haben Sie gesehen, daß die Seite eins den Platz für den Prozessor-Stack zur Verfügung stellt. Auch die Seite Null (die Zero-Page), das sind die Adressen 0 bis 255 ($00 bis $FF), hat für den Prozessor eine besondere Bedeutung. Auf sie kann nämlich mit der sogenannten direkten oder Zero-Page-Adressierung zugegriffen werden.

Im Prinzip funktioniert diese Adressierungsart genau wie die absolute Adressierung. Der Unterschied besteht darin, daß zur Angabe einer Zero-Page-Adresse nur ein Byte benötigt wird; alle anderen Adressen sind ja bekanntlich Zwei-Byte-Werte. Zu allen Befehlen, die mit der Adressierungsart „absolute" arbeiten können (bis auf den JMP-Befehl), gibt es auch eine Zero-Page-Version. In dieser Variante handelt es sich dann um Zwei-Byte-Befehle, die nicht nur um ein Byte kürzer als die gewohnten Befehle sind, sondern auch schneller abgearbeitet werden.

Im Programmtext unterscheiden sich die beiden Versionen dieser Befehle nicht. Der Assembler erkennt, daß die angegebene Adresse auf der Zero-Page liegt, und fügt bei der Übersetzung automatisch den kürzeren Maschinenbefehl ein. Die CPU erkennt bei der Abarbeitung des Programmes bekanntlich am ersten Byte eines Befehles die Instruktionslänge. So ist auch die Zero-Page-Adressierung wie alle anderen Adressierungsarten im Instruktions-Byte verschlüsselt.

Kehrseite

Die Adressen 0 und 1 der Zero-Page sind beim C64 nicht verfügbar. Das liegt daran, daß er mit einer 6510-CPU ausgestattet ist, die diese beiden Register für besondere Zwecke benutzt. Hier ist der gravierendste Unterschied zum 6502, der ja der „Vater" dieses Prozessors ist. Im C64 wird mit den Registern 0 und 1 die Speicherkonfiguration eingestellt. Dazu mehr in der nächsten Folge.

Da es sich bei der Zero-Page um einen „schnellen" Speicherbereich handelt und — wie wir noch sehen werden — die mächtigsten Adressierungsarten Platz auf der Zero-Page benötigen, werden von den 254 verfügbaren Speicherstellen die meisten vom Betriebssystem des C64 benutzt. Wenn man auf diesen Speicherbereich zugreift, muß man sich im klaren darüber sein, daß man dadurch das Betriebssystem durcheinanderbringen kann und eventuell einen Absturz des Rechners riskiert.

Unbenutzt sind in der Zero-Page nur die Adressen 2 sowie $FB bis $FE. Innerhalb unseres Simulators stehen Ihnen die Adressen $F8 bis $FF zur freien Verfügung.

Sie haben in der letzten Folge der Assembler-Schule gelernt, wie man Speicherstellen, die ein Programm zur

Parameterübergabe benötigt, an den Anfang des Programmes legt. Dadurch bleiben die Adressen auch bei einer Programmänderung konstant. Eine andere beliebte Methode, Werte an ein Programm zu übergeben, besteht darin, die Zero-Page dafür zu benutzen. Dann kann das Programm auch in einen anderen Speicherbereich assembliert werden, ohne daß sich diese Adressen ändern. Auch die Rückgabe von Ergebnissen eines Programmes erfolgt häufig über die Zero-Page.

In unserem ersten Beispielprogramm benutzen wir eine Speicherstelle der Zero-Page als Zwischenspeicher. Bevor wir diese Routine unter die Lupe nehmen, sollen Sie noch eine andere Adressierungsart kennenlernen, die dort verwendet wird. Dabei werden die Indexregister X und Y erstmals als solche benutzt. Bisher haben wir sie ja nur als Zähler eingesetzt.

Adressen plus Index

Die Adressierungsart, um die es geht, heißt „Absolut Indiziert". Bild 1 zeigt das Prinzip an einem Beispiel. Dabei enthält das X-Register eine 7. Diese Adressierungsart wird mit folgender Schreibweise gekennzeichnet:

STA $C100,X

Zu der im Befehl angegebenen Adresse wird dabei noch der derzeitige Inhalt eines der Indexregister addiert. Das Resultat dieser Addition ergibt dann die Adresse, auf den der Befehl zugreift.

Diese Adressierungsart funktioniert bei den meisten Befehlen, die mit der absoluten Adressierung arbeiten können. Eine genaue Aufstellung der Befehle mit den möglichen Adressierungsarten bringen wir in der nächsten Folge der Assembler-Schule. Sie ist auch in den Büchern enthalten, die Sie am Ende dieses Artikels aufgelistet finden. Innerhalb unseres Simulators können Sie nach dem Motto „Probieren geht über Studieren" arbeiten. Eine Adressierungsart, die für den eingegebenen Befehl nicht existiert, wird schon bei der Programmeingabe abgewiesen.

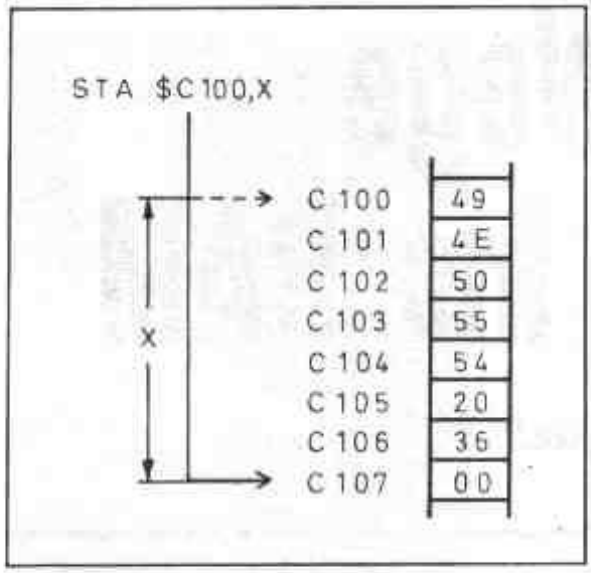


Bild 1: Bei der absolut indizierten Adressierung bildet das Index-Register den Offset

Bei den meisten Befehlen können Sie auch das Y-Register als Index verwenden. Die Notation lautet dann beispielsweise

Diese Adressierungsarten finden immer dann Verwendung, wenn in einem Speicherbereich mit jedem Byte die gleiche Operation durchgeführt werden soll. Mit ein und demselben Befehl ist es — je nach dem laufenden Inhalt des entsprechenden Index-Registers — möglich, auf 256 aufeinanderfolgende Bytes zuzugreifen. Damit lassen sich beispielsweise Tabellen bis zu dieser Länge sehr einfach verwalten.

Sie können zum Beispiel eine Schleife programmieren, die bei jedem Durchlauf das X-Register inkrementiert und dadurch jedesmal eine andere Adresse anspricht. Listing 1 zeigt eine solche Routine. Mit wenigen Befehlen kopiert sie einen Speicherbereich von 256 Bytes Länge in einen anderen.

Wenn Sie sich nun das erste Beispielprogramm auf Ihrem Datenträger anschauen, werden Sie wahrscheinlich nicht auf Anhieb die indiziert adressierten Befehle finden. Sie werden zunächst über einige bisher gänzlich unbekannte Befehle stolpern.

Namen statt Zahlen

Dabei handelt es sich nicht um neue Maschinensprache-Befehle. Es sind vielmehr Anweisungen an den Assembler. Mit ihnen werden Labels, also Assembler-Variablen, deklariert.

```
C083:   ;...
C083:   ;256 BYTES VON ORIG
C083:   ;NACH COPY KOPIEREN
C083:          LDX  #0
C085:   LOOP   LDA  ORIG,X
C088:          STA  COPY,X
C08B:          INX
C08C:          BNE  LOOP
C08E:   ;...
```

Wenn Sie diese Routine abtippen und in eigenen Programmen einsetzen, müssen die Labels ORIG und COPY vorher deklariert sein

Bislang haben wir Labels immer nur für Adressen innerhalb des Programmes benutzt. Aber ein Assembler kann sich unter einem Label-Namen beliebige Zahlen und auch Adressen außerhalb des Programmes merken und bei der Übersetzung einsetzen.

Der erste Befehl weist der Variablen RTRN die Zahl 13, das ist der ASCII-Wert der RETURN-Taste, zu. Dadurch kann überall im Programm, wo dieser Wert gebraucht wird, statt dessen der Name verwendet werden. Durch diese Maßnahme werden Programme besser lesbar. „Im richtigen Leben" kann man sich auch Label-Tabellen erstellen, die je nach Bedarf beim Programmieren in den Text geladen werden. Sie können sich auf diese Weise eine Menge Tipparbeit sparen.

Die nächsten vier Befehle haben denselben Sinn: DELC erhält den Wert der DEL-Taste, LEER den der Leertaste, LEFT steht im Programm für Cursor-Links, und unter CRSR steht ein Grafikzeichen zur Verfügung, das in der Routine als Cursor dient.

Bei dem vorgestellten Programm handelt es sich um eine Routine, die Sie auch in eigene Programme einfügen können. Sie enthält einen simplen Zeilen-Editor. Man kann mit ihr bis zu 255 Zeichen von der Tastatur holen und in einem Speicherbereich ablegen. Das jeweils zuletzt eingegebene Zeichen ist mit der DEL-Taste zu löschen.

Die Zero-Page-Adresse $FE wird durch die folgende Anweisung mit dem Label MERK versehen. Sie wird als schneller Zwischenspeicher für das X-Register dienen.

Der Beginn des Bereiches, in dem der eingegebene String gespeichert werden soll, ist im Programm durch das Label BUFF gekennzeichnet. Das bewirkt die Zeile

BUFF = $C100

Dadurch, daß auch diese Adresse in einer Assembler-Variablen gehalten wird, brauchen Sie später bei Bedarf nur diese Zeile zu ändern, und die Routine benutzt einen anderen Bereich als Puffer.

INPUT selbstgemacht

Der erste eigentliche Befehl — unter der Überschrift — initialisiert das Index-X-Register. Sein Inhalt wird dann für später in die Speicherstelle MERK gerettet. Beachten Sie die Instruktionslänge von nur zwei Bytes — MERK liegt auf der Zero-Page.

Im nächsten Befehl sehen Sie, wie auf die zu Anfang vereinbarten Namen zugegriffen wird: Der Assembler setzt bei der Übersetzung für CRSR wieder 164 ein, und im Trace-Protokoll wird der Befehl als LDA #$A4 auftauchen.

Ab EIN1 wird die Tastatur abgefragt; diesen Mechanismus haben Sie ja in der letzten Folge schon kennengelernt. Ist ein Tastendruck erfolgt, so wird das X-Register wieder mit seinem alten Wert geladen. Die Routine GETC könnte es verändert haben (siehe Kasten).

Falls es sich bei dem eingegebenen Zeichen um ein RETURN handelt, verzweigt das Programm nach RAUS, die DEL-Taste bewirkt einen Sprung nach DELT. Andere Sonderzeichen werden durch die Befehle $C01D bis $C023 abgewiesen. Der folgende Befehl gibt das empfangene Zeichen als Echo auf dem Bildschirm aus.

Jetzt kommt das eigentlich Spannende an diesem Programm: Der Befehl

STA BUFF,X

speichert das empfangene Zeichen ab. Durch die Verwendung der X-indizierten Adressierung und den nachfolgenden INX-Befehl wird das erste Zeichen an der Adresse $C100 abgespeichert, das nächste bei $C101 und so weiter. Ein Speicherbereich, der mit der indizierten Adressierung erreicht werden soll, muß übrigens nicht immer auf der ersten Adresse einer Seite beginnen; die Basis-Adresse ist beliebig.

Der folgende Branch-Befehl wacht darüber, daß nicht mehr als 255 Zeichen eingegeben werden. Wenn nämlich der INX-Befehl eine Null ergibt, würde das nächste Zeichen direkt auf der Speicherstelle BUFF abgespeichert werden. Der Sprung nach DEL1 bewirkt, daß das 256. eingegebene Zeichen sofort wieder gelöscht wird.

Ist das Ende des Puffers noch nicht erreicht, so wird der folgende Branch-Befehl wirksam, und das Programm wartet auf die nächste Taste.

Ergänzungen und Berichtigungen

Solange Sie im Simulator arbeiten, merken Sie es nicht, aber wenn Sie ein Programm, das die Betriebssystem-Routine GETC benutzt, abspeichern, assemblieren und unter echten Bedingungen laufen lassen, passiert es: Die „wahre" GETC-Routine im ROM des C64 verändert die Index-Register X und Y. Die Programme 1 und 4 aus der letzten Folge laufen daher nicht in der veröffentlichten Form.

Falls Sie sie trotzdem benutzen wollen, können Sie das erste Programm aus dieser Folge als Muster nehmen: Speichern Sie den Inhalt der noch benötigten Index-Register vor dem Aufruf von GETC irgendwo ab, und holen Sie ihn hinterher wieder zurück.

Das Label RAUS ist der Anfang vom Ende der Routine: Zuerst wird das Ende des eingegebenen Strings mit einem Null-Byte markiert. Für diese Markierung könnte man auch einen anderen Wert benutzen, die Null hat sich aber nun mal eingebürgert. Der BASIC-Interpreter macht es genauso, und das zweite Programm — das der Textausgabe dienen wird — verwendet dieses Kennzeichen auch.

Die folgenden Befehle entfernen den Cursor vom Bildschirm, springen in die nächste Textzeile, und der RTS-Befehl schließlich übergibt die Kontrolle wieder dem aufrufenden Programm. Ihn können Sie zu Testzwekken innerhalb des Kurses durch ein BRK ersetzen, dann bleiben Sie im Simulator und können noch Speicherbereiche inspizieren.

Indexvergleiche

Der Rest des Programmes dient dem Löschen des letzten Zeichens. Der Befehl

CPX

ist neu. Er bedeutet ComPare to X-register und bewirkt dasselbe wie der in Lektion 2 beschriebene CMP-Befehl. Der Unterschied besteht darin, daß das Argument nicht mit dem Inhalt des Akkumulators, sondern mit dem X-Register verglichen wird. Mit Ihrer Vermutung, daß es auch einen Befehl namens CPY gibt, haben Sie übrigens recht.

Mit dem CPX-Befehl überprüft unser Programm vor dem Löschen eines Zeichens, ob überhaupt schon eins eingegeben wurde.

Die restlichen Befehle bewirken neben der Cursor-Bewegung eine Dekrementierung des X-Registers. Dadurch wird zwar das letzte Zeichen nicht wirklich aus dem Speicher gelöscht. Die nächste Eingabe wird es jedoch überschreiben.

Kurz und gut

Der Vollständigkeit halber sei hier erwähnt, daß auch auf die Zero-Page indiziert zugegriffen werden kann. Alle Befehle, die mit der Adressierung „absolut,X" funktionieren, können auch in der Version „Zero-Page,X" eingesetzt werden. Ferner kennt die 6502-CPU noch die Adressierungsart „Zero-Page,Y". Sie ist allerdings den Befehlen LDX und STX vorbehalten.

Wegen des bereits erwähnten Gedränges, das auf der Seite Null herrscht, wird diese Möglichkeit des Prozessors beim C64 verhältnismäßig selten genutzt. Größere Tabellen werden normalerweise nicht in der Zero-Page aufbewahrt. Bei kleineren 6502-Systemen wie dem EPAC65 unserer Schwesterzeitschrift c't, die ohne aufwendiges Betriebssystem auskommen, sind diese Adressierungen jedoch wegen der Platz- und Zeitersparnis durchaus üblich.

Mit Klammer

Die mächtigsten Adressierungsarten, die die 6502-CPU zur Verfügung stellt, imponieren schon durch ihre Namen: Sie heißen „indiziert indirekt" und „indirekt indiziert". Man spricht auch von Vor- beziehungsweise Nach-Indizierung. Beiden ist gemeinsam, daß sie Zeiger (neudeutsch Pointer) auf der Zero-Page benutzen. Dazu kommt noch jeweils ein Index-Register. Alle Befehle, die diese Adressierungsarten benutzen, sind zwei Bytes lang (Instruktionsbyte und Zero-Page-Adresse).

Ein Zeiger besteht aus zwei aufeinanderfolgenden Bytes, die eine Adresse enthalten. Dabei steht der niederwertige Teil der Adresse (das Low-Byte) im ersten, der höherwertige (High-Byte) im zweiten Byte. Diese Reihenfolge — Sie kennen sie ja schon von der Assembler-Anweisung W — ist beim 6502 überall anzutreffen. (Beispielsweise wird auch die Adresse bei einem Drei-Byte-Befehl in dieser Reihenfolge erwartet — aber darum kümmert sich der Assembler.)

Die Adressierungsart „indiziert indirekt" benutzt zusätzlich zu dem Pointer auf der Zero-Page noch das X-Register. Die Funktionsweise dieser Adressierung soll die linke Hälfte von Bild 2 erklären. Wir setzen voraus,

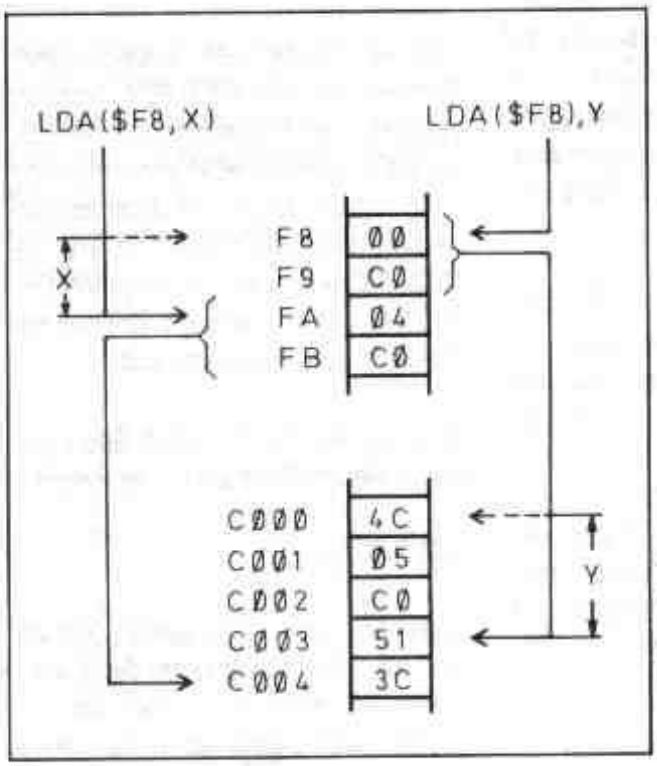


Bild 2: Die mächtigsten Adressierungsarten des 6502 benutzen eine Kombination von Zero-Page-Pointer und Index-Register zur Adreßberechnung.

daß das X-Register den Wert 2 enthält. Die Schreibweise lautet

LDA (SF8,X)

Der Prozessor addiert zunächst den Inhalt des X-Registers zu der angegebenen Adresse. Die beiden an der dadurch angegebenen und der folgenden Zero-Page-Adresse stehenden Bytes werden als Pointer auf die Adresse aufgefaßt, auf die die CPU schließlich zugreift.

Mit dieser Adressierung kann man auf der Zero-Page Adreßtabellen anlegen, auf die sehr leicht zugegriffen werden kann. Wegen der Überfüllung auf der Seite Null ist beim C64 auch diese Adressierungsart eher selten.

Wesentlich bedeutender ist die nachindizierte Adressierung. Sie benutzt das Index-Y-Register. Auf der rechten Seite von Bild 2 ist dargestellt, wie sie wirkt. Das Y-Register enthält in unserem Beispiel den Wert 3.

Die CPU holt sich aus der angegebenen und der folgenden Adresse einen Pointer. Zu diesem addiert sie den Inhalt des Y-Registers und bildet so die anzusprechende Adresse.

Diese Adressierungsart hat mehrere entscheidende Vorteile: Mit nur einem Zero-Page-Pointer kann durch unterschiedlichen Inhalt des Y-Registers ein Bereich von 256 Bytes adressiert werden. Der Beginn dieses Bereiches kann innerhalb des Programmes berechnet werden und ist nicht unbedingt vom Programmierer fest vorzugeben.

Jede Menge Labels

In der Routine PRNT des zweiten Beispielprogrammes wird von dieser Adressierungsart Gebrauch gemacht. Sie dient dazu, einen String mit bekannter Anfangsadresse auf dem Bildschirm auszugeben.

Zum Programm

Die INPUT 64-Assembler-Schule setzt sich aus mehreren Teilen zusammen. Nach dem Laden sehen Sie ein Titelbild, von dem aus Sie mit einem beliebigen Tastendruck in das Hauptmenü gelangen.

Wenn Sie nun F1 drücken, gelangen Sie in ein Menü, das Ihnen verschiedene Themen zur Auswahl stellt. Die Erklärungen, die Sie jetzt abrufen können, sollten Sie parallel zum Beiheft lesen. Beide Medien ergänzen sich hier. Sie können die Erklärungen auch mit CTRL-B ausdrucken. Ins Hauptmenü gelangen Sie jederzeit mit der STOP-Taste zurück.

Mit F3 gelangen Sie aus dem Hauptmenü zu einer Auswahl verschiedener Beispielprogramme. Sie können eines davon auswählen, das Sie sich dann im Editor anschauen oder auch verändern können. Wenn Sie an dieser Stelle eine Null eingeben, enthält der Editor das zuletzt bearbeitete Programm, beim ersten Aufruf ist der Textspeicher leer.

Wenn Sie ein Beispielprogramm bearbeitet haben und — mit der STOP-Taste — wieder ins Hauptmenue springen, können Sie Ihren Text auch auf einen Drucker ausgeben lassen oder auf einen eigenen Datenträger abspeichern. Abgespeicherte Programme können Sie direkt mit dem INPUT-ASS (Ausgabe 6/86) laden und weiterbearbeiten.

Vom Editor aus gelangen Sie mit F7 in einen integrierten Simulator. Hier können Sie unsere Programmbeispiele oder Ihre selbstentworfenen Programme ablaufen lassen und testen, ob sie sich erwartungsgemäß verhalten.

Ausführliche Hinweise zur Bedienung des Editors und des Simulators sind im Programm enthalten. Sie können Sie von dort aus jeweils mit der Funktionstaste F6 aufrufen. Es wird empfohlen, diese Seiten vor der Benutzung des Programmpakets einmal gründlich zu lesen. Besitzer eines Druckers können sie auch mit CTRL-B zu Papier bringen.

Die INPUT 64-Assembler-Schule ist eine Serie, die in Ausgabe 3/87 begonnen hat. Die einzelnen Lektionen bauen aufeinander auf. Wer noch keine Erfahrungen mit der Maschinensprache-Programmierung hat, tut gut daran, mit der ersten Folge anzufangen.

Das Programm beginnt mit zwei Label-Zuweisungen. PTRL und PTRH sind zwei aufeinanderfolgende Adressen auf der Zero-Page; sie werden als Pointer auf den auszugebenden Text dienen. ANZT ist eine reine Assembler-Variable und enthält die Anzahl der verschiedenen möglichen Texte.

Schauen wir uns noch die letzten Programmzeilen an, bevor das eigentliche Programm auseinandergenommen wird. Hier stehen die verschiedenen Texte, die das Programm ausgeben kann. Der Befehl B ist eine Assembler-Anweisung. Wir haben sie schon öfter benutzt, um bestimmte Speicherstellen mit einem Wert vorzubesetzen. Trifft der Assembler bei der Übersetzung hinter der B-Anweisung auf Texte in Anführungszeichen, so setzt er die entsprechenden ASCII-Werte in den Programmspeicher ein.

In den Tabellen TABL und TABH sind die nieder- beziehungsweise die höherwertigen Bytes der Anfangsadressen der Texte gespeichert. Ein Kleiner-Zeichen vor einem Argument signalisiert dem Assembler, daß er das niederwertige Byte des folgenden Wertes erzeugen soll, ein Größer-Zeichen ergibt das höherwertige Byte.

Das Label TXTN haben wir noch vergessen; hier ist die Nummer des auszugebenden Textes gespeichert. Wenn Sie andere Texte einsetzen und ein Programm schreiben, das diese Nummer irgendwie berechnet, können Sie das vorliegende Programm zur Ausgabe beliebiger Meldungen verwenden

PRINT Marke Eigenbau

Das eigentliche Programm beginnt damit, daß es die Nummer des Textes ins X-Register lädt, und prüft, ob ein solcher Text überhaupt vorhanden ist. Falls ja, wird das X-Register als Index auf die beiden Text-Tabellen benutzt und die Anfangsadresse des Textes in den Akku und das Y-Register geladen.

Werfen wir nun einen Blick auf die Routine PRNT. Sie erwartet die Anfangsadresse des auszugebenden Textes im Akku und im Y-Register, und zwar das Low-Byte im Akku und das High-Byte im Y-Register. Diese Adresse wird als Pointer in der Zero-Page abgespeichert. Unter Benutzung der indirekt-indizierten Adressierung wird der String nun Byte für Byte ausgelesen und an die Betriebssystem-Routine PRCH übergeben. Diese Routine arbeitet so lange, bis sie auf eine Null trifft oder 256 Zeichen ausgegeben sind.

Zurück zur Adresse $C01D: Hier landet das Programm, wenn das Byte TXTN einen ungültigen Wert enthält. Dann wird die Adresse des Textes ERRT auf die bekannte Art und Weise an PRNT übergeben.

Auf eigenen Füßen

Abschließend gibt das Programm in jedem Falle noch ein Ausrufezeichen aus und wartet auf einen Tastendruck, bevor es zur Aufruf-Adresse zurückkehrt.

Dieses Programm bietet mannigfaltige Möglichkeiten zum Experimentieren. Das einfachste ist, die Zahl bei TXTN zu ändern und dadurch einen anderen der vorhandenen Texte ausgeben zu lassen. Sie können aber auch die Texte selbst oder die Anzahl der Texte ändern. Wenn Sie das Programm in Eigenentwicklungen integrieren wollen, sollten Sie die Befehle, die abschließend auf einen Tastendruck warten, entfernen. Bestimmt fällt Ihnen auch eine Anwendung ein, bei der Sie die beiden in dieser Folge vorgestellten Programme zu einem verbinden.

In der nächsten Folge werden wir die noch fehlenden Maschinensprache-Befehle vorstellen und eine komplette Aufstellung der Befehle und der möglichen Adressierungsarten bringen. Außerdem werden wir einige C64-Besonderheiten besprechen.

Hajo Schulz

Literatur

Christian Persson: 6502/65C02-Maschinensprache. Verlag Heinz Heise GmbH, Hannover 1983

Rodnay Zaks: Programmierung des 6502. Sybex-Verlag GmbH, Düsseldorf 1981

Stapelweise Befehle

INPUT 64-Assembler-Schule, Teil 5

Wenn Sie sich die Opcode-Tabelle in der Mitte dieses Heftes ansehen, werden Sie feststellen, daß Sie die meisten Befehle schon kennen. Wir haben zwar nicht jeden Befehl mit jeder Adressierungsart verwendet. Die Arbeitsweise der Befehle sollte Ihnen aber trotzdem bekannt sein. Es ist übrigens ziemlich überflüssig, diese Tabelle auswendig zu lernen, Sie sollten aber wissen, welche Befehle mit welchen Adressierungsarten kombinierbar sind.

Wenn Sie die bisherigen Folgen dieses Kurses aufmerksam durchgearbeitet haben, sind Sie in Maschinensprache schon einigermaßen fit. Die wenigen Befehle, die Sie noch nicht kennengelernt haben, werden diesmal besprochen. Außerdem wollen wir einen Blick auf Eigenheiten des C64 werfen.

Faulenzer

Der einfachste unter den Befehlen, die wir noch nicht vorgestellt haben, heißt

NOP

Er benötigt keine Argumente und tut auch nichts (NOP heißt No OPeration — keine Operation). Auf den ersten Blick scheint es überflüssig, einen solchen Befehl zur Verfügung zu haben. Aber auch das Nichtstun kostet Zeit. Und manchmal kommt es eben darauf an, die CPU ein wenig warten zu lassen, ohne Registerinhalte zu verändern. Der Befehl findet häufig in zeitkritischen Routinen Anwendung, zum Beispiel bei Programmen zur Bedienung des Kassettenrecorders oder der seriellen Schnittstelle.

Bit-Tester

Ebenfalls bei Programmen, die für Peripherie zuständig sind, wird der Befehl

BIT

gern verwendet. Mit ihm kann abgefragt werden, ob bestimmte Bits in der angesprochenen Speicherstelle gesetzt sind. Er führt eine bitweise AND-Verknüpfung zwischen dem Akku und dem Inhalt der Adresse durch. Im Gegensatz zum AND-Befehl wird das Resultat jedoch nicht in den Akku übernommen. Sein Inhalt bleibt unverändert — etwas Ähnliches kennen Sie ja schon von dem Befehl CMP.

Je nach dem Ergebnis der AND-Verknüpfung wird die Z-Flagge im Statusregister gesetzt. Die Flags N und V enthalten nach der Abarbeitung des BIT-Befehls den Inhalt der Bits 7 beziehungsweise 6 der getesteten Adresse.

Mit diesem Befehl kann man also unabhängig vom Akku-Inhalt die beiden obersten Bits eines Speicher-Bytes testen. Will man andere Bits überprüfen, so muß der Akku vorher mit einer entsprechenden Maske geladen werden.

Speicher als Zähler

Auch die beiden Befehle, die jetzt zur Sprache kommen sollen, sind nicht schwer zu verstehen; sie arbeiten ähnlich wie schon bekannte Kommandos. Gemeint sind

INC (INCrement memory) und
DEC (DECrement memory).

Der Befehl INC tut dasselbe wie INX oder INY, nur wird nicht ein Indexregister, sondern eine Speicherstelle um eins erhöht. Die Flaggen des Statusregisters verhalten sich dabei wie gehabt.

Der DEC-Befehl vermindert den Inhalt der angesprochenen Adresse um eins, auch er beeinflußt die N- und die Z-Flagge wie die Befehle DEX und DEY.

Diese beiden Befehle werden benutzt, wenn ein Schleifenzähler benötigt wird, aber die Register X und Y als Indexregister verwendet werden müssen. Eine andere Anwendung dieser Befehle zeigt Bild 1. Hier wird mit dem INC-Befehl Zeit und Speicherplatz gespart. Bei der Subtraktion einer Ein-Byte-Zahl von einem Zwei-Byte-Wert können Sie mit dem DEC-Befehl den gleichen Trick anwenden.

Datenkeller

In der vorletzten Folge haben Sie den Prozessor-Stack, auch Kellerspeicher genannt, kennengelernt. Sie kennen seine Bedeutung für die Aufbewahrung von Rückkehradressen bei Un-

```
C018:  ;PNTR=PNTR+7
C018:        CLC
C019:        LDA PNTR
C01C:        ADC #7
C01E:        STA PNTR
C021:        LDA PNTR+1
C024:        ADC #0
C026:        STA PNTR+1
C029:        ...
```

```
C018:  ;PNTR=PNTR+7
C018:        CLC
C019:        LDA PNTR
C01C:        ADC #7
C01E:        STA PNTR
C021:        BCC OKAY
C023:        INC PNTR+1
C026:  OKAY  ...
```

Bild 1: Mit dem INC-Befehl wird die Adition eines Bytes zu einem Zwei-Byte-Wert schneller und kürzer.

terprogrammaufrufen. Das ist aber nur die halbe Wahrheit. Man kann den Stack nämlich auch selbst für die Zwischenspeicherung beliebiger Daten nutzen. Dazu gibt es das Befehlspaar

PHA (PusH Accu) und
PLA (PulL Accu).

Der erste dieser beiden Befehle „schiebt" den Inhalt des Akkus auf den Stapel. Dabei wird der Stackpointer um eins vermindert, diese Operation belegt also nur ein Byte im Stack. (Beim JSR-Befehl sind es jedesmal zwei Bytes.)

Durch den PLA-Befehl wird der so zwischengespeicherte Wert wieder in den Akku zurückgeholt und der belegte Speicherplatz im Stapel freigegeben.

Diese beiden Befehle sind mit äußerster Vorsicht zu genießen. Vergißt man nämlich, einen gePUSHten Wert zurückzuholen, oder läßt den Prozessor einen überflüssigen PLA-Befehl ausführen, so befindet sich der Stack in einem nicht ordnungsgemäßen Zustand — und das nächste RTS kommt bestimmt. Der Prozessor kann ja nicht wissen, ob die beiden oben auf dem Stack liegenden Bytes durch einen PHA- oder durch einen JSR-Befehl dort hingekommen sind. Er interpretiert sie bei einem RTS immer als Return-Adresse. Und daß dieser Sprung „in die Wüste" geht, wenn ein Byte zuviel oder zuwenig auf dem Stack liegt, dürfte wohl klar sein. Diesem Programmierfehler ist besonders schwer beizukommen, da der Prozessor dabei jedesmal woanders landen kann und sich unter Umständen völlig chaotisch verhält.

Leider gibt es die Möglichkeit der Ablage auf dem Stack nicht für die Indexregister. Braucht man sie doch einmal, muß man sich mit einer TXA-PHA- beziehungsweise PLA-TAX-Folge behelfen. (Achtung, dabei geht der Akku-Inhalt verloren!)

Zum Trost haben die Entwickler des 6502 die Möglichkeit vorgesehen, den Inhalt des Prozessor-Status-Registers auf dem Stack abzulegen und wiederherzustellen. Dazu gibt es die Befehle

PHP (PusH Processor status) und
PLP (PulL Processor status).

Auch diese beiden Befehle sind nicht ganz ungefährlich. Zusätzlich zu den bei PHA und PLA besprochenen Problemen kann ein unüberlegtes PLP-Kommando beispielsweise dazu führen, daß plötzlich die D-Flagge gesetzt ist und keiner weiß, warum das Programm nur noch Müll berechnet.

Andererseits sind diese beiden Befehle die einzigen, mit denen man direkt an das Statusregister herankommt. Um zu testen, ob die D-Flagge gesetzt ist, muß man zum Beispiel die Befehlsfolge

```
PHP
PLA
AND #%00001000
BEQ HEXA
BNE DEZI
```

verwenden. Es gibt nämlich keinen BDS- („Branch on Decimal Set"-) Befehl.

Das Unterste zuoberst kehren

Wo wir gerade beim Stack sind, sollen hier noch zwei Befehle vorgestellt werden, die auch mit dem Keller zu tun haben. Sie heißen

TSX (Transfer Stack pointer to X) und
TXS (Transfer X to Stack pointer).

Letzterer dient dazu, den Stackpointer zu initialisieren. Das muß zum Beispiel beim Einschalten des Rechners oder nach einem Reset geschehen. Dazu wird das X-Register normalerweise mit $FF geladen und dann der TXS-Befehl ausgeführt. Dadurch sind aus der Sicht des Prozessors alle Eintragungen aus dem Stack entfernt, und es stehen wieder 256 freie Plätze zur Verfügung.

Der TSX-Befehl ist die einzige Möglichkeit, den Inhalt des Stackpointers zugänglich zu machen. Der BASIC-Interpreter prüft zum Beispiel vor jedem GOSUB-Befehl mit einer TSX-CPX-Folge, ob noch genug Platz auf dem Stapel frei ist.

Mit diesem Befehl kann man auch die Kellerstruktur überlisten und zum Beispiel die drittletzte Eintragung aus dem Stack lesen:

```
TSX
LDA $103,X
```

Dabei wird weder der Stackpointer noch der Inhalt des Stapels selbst beeinflußt.

Anlasser

Alle Befehle und Programme, die wir bislang besprochen haben, arbeiten genau voraussehbar. Das heißt, wenn man die Registerinhalte des Prozessors und das Programm kennt, kann man genau voraussagen, welche Aktionen in welcher Reihenfolge durchgeführt werden. Es gibt aber auch Möglichkeiten, diese Abarbeitung eines Programmes von außen zu beeinflussen. Dazu gibt es die sogenannten Unterbrechungen oder Interrupts.

Beim 6502 gibt es drei Arten, von außen eine Programmunterbrechung herbeizuführen. Eine davon ist der Reset. Der Prozessor hat dafür eine spezielle Leitung. Wird an dieser ein Impuls angelegt, so bricht der Prozessor sofort seine Arbeit ab. Er lädt dann den Programmzähler mit dem Inhalt der Adressen $FFFC und $FFFD. Diese Adressen liegen im ROM. Das ist bei jedem 6502-Rechner so, denn auch beim Einschalten wird der Programmzähler mit dieser Adresse geladen, und die soll ja jedesmal denselben Wert enthalten, damit der Computer in einen definierten Ausgangszustand kommt.

Das Laden des Programmzählers mit der Reset-Adresse bewirkt nichts anderes als einen Sprung zu dieser Adresse. Beim C64 ist es die Adresse $FCE2 (64738). An dieser Stelle (auch noch im ROM) steht eine Routine, die zunächst den Stackpointer initialisiert, die D-Flagge löscht und überprüft, ob ein Autostart-Modul im Extension-Port steckt. Falls nicht, werden als nächstes die Peripherie-Chips initialisiert. Dazu gehört zum Beispiel, daß Hintergrund- und Rahmenfarbe gesetzt werden, die Lautstärke des SID auf null geht und die Schnittstellen (Userport, serieller Bus, Kassette etc.) in einen definierten Zustand versetzt werden.

Dann werden diverse Pointer und Vektoren gesetzt. (Zu dem Begriff Vektoren kommen wir in wenigen Augenblicken.) Zum Schluß wird die NEW-Routine angesprungen, und von da aus geht es in den BASIC-Interpreter, der nun auf Ihre Eingaben wartet.

Unterbrechungen . . .

Die beiden anderen erwähnten Hardware-Unterbrechungen heißen „nicht maskierbarer Interrupt" (NMI) und Interrupt-Anfrage („Interrupt-Request", IRQ). Sie laufen ganz ähnlich ab wie ein Reset, dienen aber anderen Zwecken. Mit ihnen kann ein laufendes Programm unterbrochen werden, damit der Prozessor zwischendurch etwas anderes tut und dann zum unterbrochenen Programm zurückkehrt.

Beim C64 wird zum Beispiel regelmäßig ein IRQ ausgelöst, und zwar sechzigmal pro Sekunde. Das heißt, jedes Programm wird alle sechzigstel Sekunde unterbrochen. Der Prozessor führt dadurch regelmäßig ein Programm aus, das überprüft, ob eine Taste gedrückt ist, den Cursor blinken läßt, die Zeit (TI$) hochzählt und beim Drücken der STOP-Taste ein BASIC-Programm abbricht. Diese Routine läuft quasi „im Hintergrund", der Anwender merkt überhaupt nicht, daß sein Programm laufend unterbrochen wird.

Die Rückkehr zum unterbrochenen Programm wird dadurch bewerkstelligt, daß die CPU bei einem Interrupt ähnlich reagiert wie bei einem Unterprogrammaufruf. Die Adresse des nächsten Befehles wird nämlich auf dem Stack abgelegt.

Zusätzlich speichert der Prozessor auch den Inhalt des Statusregisters auf dem Stack ab. Denn im Gegensatz zu einem JSR-Befehl weiß man ja als Programmierer nicht, wann während des Programmlaufes ein Interrupt ausgelöst wird. Kommt er zufällig zwischen einem CMP- und einem BEQ-Befehl und verändert die Interrupt-Routine die Zero-Flagge, könnte das fatale Folgen haben.

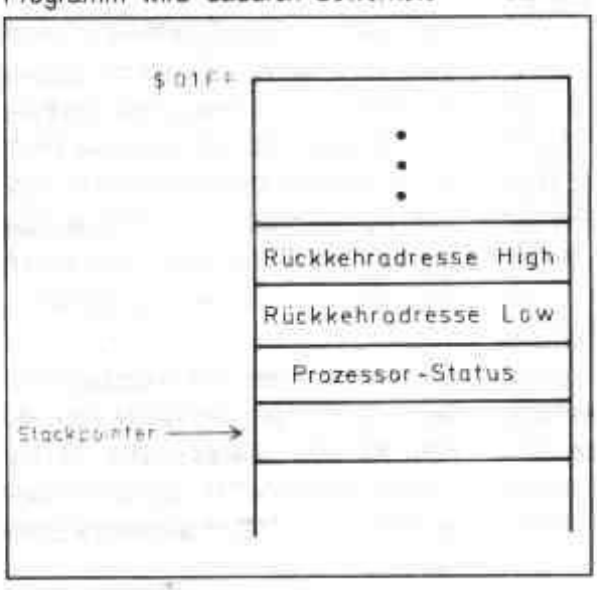
Zur Rückkehr in das unterbrochene Programm dient der Befehl

RTI (ReTurn from Interrupt),

der die Rückkehradresse und den Inhalt des Statusregisters wieder vom Stack holt.

. . .und wie man sich dagegen wehrt

Der Unterschied zwischen einem NMI und einem IRQ besteht darin, daß ein NMI in jedem Falle zu einer Programmunterbrechung führt, während man den IRQ unterbinden kann. Dazu dient die I-Flagge des Statusregisters. Sie kann mit dem Befehl



Bei einer Unterbrechung wird zuerst die Rückkehradresse, dann das Statusregister auf den Stack gerettet.

Zum Programm

Die INPUT 64-Assembler-Schule setzt sich aus mehreren Teilen zusammen. Nach dem Laden sehen Sie ein Titelbild, von dem aus Sie mit einem beliebigen Tastendruck in das Hauptmenü gelangen.

Wenn Sie nun F1 drücken, gelangen Sie in ein Menü, das Ihnen verschiedene Themen zur Auswahl stellt. Die Erklärungen, die Sie jetzt abrufen können, sollten Sie parallel zum Beiheft lesen. Beide Medien ergänzen sich hier. Sie können die Erklärungen auch mit CTRL-B ausdrucken. Ins Hauptmenü gelangen Sie jederzeit mit der STOP-Taste zurück.

Mit F3 gelangen Sie aus dem Hauptmenü zu einer Auswahl verschiedener Beispielprogramme. Sie können eines davon auswählen, das Sie sich dann im Editor anschauen oder auch verändern können. Wenn Sie an dieser Stelle eine Null eingeben, enthält der Editor das zuletzt bearbeitete Programm, beim ersten Aufruf ist der Textspeicher leer.

Wenn Sie ein Beispielprogramm bearbeitet haben und — mit der STOP-Taste — wieder ins Hauptmenü springen, können Sie Ihren ÇText auch auf einen Drucker ausgeben lassen oder auf einen eigenen Datenträger abspeichern. Abgespeicherte Programme können Sie direkt mit dem INPUT-ASS (Ausgabe 6/86) laden und weiterbearbeiten.

Vom Editor aus gelangen Sie mit F7 in einen integrierten Simulator. Hier können Sie unsere Programmbeispiele oder Ihre selbstentworfenen Programme ablaufen lassen und testen, ob sie sich erwartungsgemäß verhalten.

Ausführliche Hinweise zur Bedienung des Editors und des Simulators sind im Programm enthalten. Sie können Sie von dort aus jeweils mit der Funktionstaste F6 aufrufen. Es wird empfohlen, diese Seiten vor der Benutzung des Programmpakets einmal gründlich zu lesen. Besitzer eines Druckers können sie auch mit CTRL-B zu Papier bringen.

Die INPUT 64-Assembler-Schule ist eine Serie, die in Ausgabe 3/87 begonnen hat. Die einzelnen Lektionen bauen aufeinander auf. Wer noch keine Erfahrungen mit der Maschinensprache-Programmierung hat, tut gut daran, mit der ersten Folge anzufangen.

SEI (SEt Interrupt disable)

gesetzt werden. Dadurch wird die Annahme des Interrupt-Requests verhindert. Um den Interrupt wieder zuzulassen, muß das I-Flag gelöscht werden. Dazu dient der Befehl

CLI (CLear Interrupt disable).

Ist die I-Flagge gelöscht, so ist die Reaktion auf einen IRQ die gleiche wie auf einen NMI. Im einzelnen passiert dabei folgendes: Zuerst wird der gerade in der Abarbeitung befindliche Befehl vollständig ausgeführt. Dann rettet der Prozessor die Rückkehradresse und das Statusregister auf den Stack und setzt die I-Flagge. Damit ist zunächst die Annahme eines weiteren IRQ gesperrt. Abschließend wird die Einsprungadresse der Interrupt-Routine aus dem ROM in den Programmzähler geladen und damit — genau wie bei einem Reset — die Interrupt-Behandlungs-Routine angesprungen.

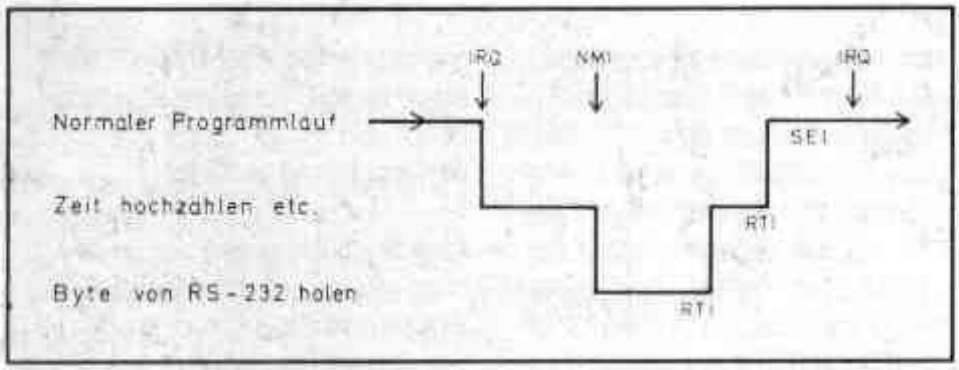
Die Adresse, an der die IRQ-Routine beginnt, steht in den Speicherzellen $FFFE und $FFFF, die für den NMI bei $FFFA und $FFFB.

Beim C64 wird ein NMI durch den gleichzeitigen Druck auf die Tasten RUN/STOP und RESTORE ausgelöst. Er dient als „weicher Reset". Außerdem kann über eine am User-Port angeschlossene RS-232-Schnittstelle ein NMI ausgelöst werden.

Wie schon erwähnt, wird ein IRQ regelmäßig durch einen Timer in einem der beiden Schnittstellenbausteine (CIAs) ausgelöst. Aber es gibt im 64er noch andere Interrupt-Quellen. So können die CIAs so programmiert werden, daß sie beim Empfangen eines Bytes am seriellen Port oder beim Anlegen eines bestimmten Spannungspegels an einer speziellen Leitung einen IRQ auslösen. Das wird zum Beispiel beim Laden von der Datassette ausgenutzt. Auch der VIC (der für die Bilderzeugung zuständige Chip) kann IRQs auslösen, beispielsweise, wenn zwei Sprites sich berühren oder wenn der Elektronenstrahl auf der Bildröhre eine bestimmte Position erreicht.

Umleitung

Nun wäre es unsinnig, auf all diese Ereignisse in derselben Art und Weise zu reagieren. Darum enthalten die NMI- und die IRQ-Routine ziemlich am Anfang einen indirekten Sprungbefehl. Das ist ein JMP-Befehl, dessen Argument nicht direkt die Adresse ist, zu der gesprungen wird, sondern eine Adresse, an der diese Adresse steht.



Ein NMI kann die IRQ-Routine unterbrechen, aber nicht umgekehrt. Er hat die höhere Priorität.

Die IRQ-Routine enthält zum Beispiel den Befehl

JMP ($0314).

Wenn die CPU auf diesen Befehl trifft, springt sie nicht zu der Adresse $314, sondern holt sich die Sprungadresse aus den Speicherzellen $314 und $315 (788/789). Man sagt, diese Adressen enthalten den IRQ-Vektor. Normalerweise steht dort die Adresse $EA31, der Beginn der IRQ-Routine im ROM.

Will man nun Interrupts für eigene Anwendungen einsetzen, so muß man diesen Vektor auf seine eigene Interrupt-Behandlungsroutine „verbiegen". Wie das geht und was dabei zu beachten ist, können Sie einem ausführlich kommentierten Assembler-Quelltext entnehmen, den Sie aus dem Programm heraus abspeichern und mit dem INPUT-ASS wieder laden können. Es handelt sich dabei um ein Programm, das den VIC so programmiert, daß er beim Erreichen einer bestimmten Rasterzeile einen Interrupt auslöst. Die Interrupt-Routine schaltet dann die Hintergrund-Farbe um.

Auf der Speicherseite drei, genauer: auf den Adressen von $300 bis $33E, stehen übrigens noch andere Sprungvektoren. Mit Ihnen ist es möglich, alle wichtigen Routinen des C64-Betriebssystems auf eigene Programme umzuleiten. Damit kann man BASIC-Erweiterungen einbinden oder die Drucker-Ausgabe auf eine Centronics-Schnittstelle am Userport umleiten. Einige dieser Vektoren sollen in der nächsten Folge der Assembler-Schule vorgestellt werden.

Dann werden wir uns auch mit der Einbindung von Assembler-Routinen in BASIC-Programme beschäftigen und einen Blick auf die Programmierung von C64-Spezialitäten wie Joystick-Abfrage und Grafik werfen. Hajo Schulz

Literatur

Christian Persson: 6502/65C02-Maschinensprache, Verlag Heinz Heise GmbH, Hannover 1983

Rodnay Zaks: Programmierung des 6502, Sybex-Verlag GmbH, Düsseldorf 1981

Alle 6502-Befehle und Adressierungsarten

Adressierungsart	Implied	Immed.	Absolut	Zero-P.	ZP,X	Abs,X	Abs,Y	(ZP,X)	(ZP),Y	Relativ	Beeinflußte Flags
Befehlslänge	1	2	3	2	2	3	3	2	2	2	NV-BDIZC
ADC		69	6D	65	75	7D	79	61	71		NV....ZC
AND		29	2D	25	35	3D	39	21	31		N.....Z.
ASL	0A		0E	06	16	1E					N.....ZC
BCC										90	....
BCS										B0	....
BEQ										F0	....
BIT			2C	24							NV....Z.
BMI										30	....
BNE										D0	....
BPL										10	....
BRK	00										...1.1..
BVC										50	....
BVS										70	....
CLC	18										0
CLD	D8										....0...
CLI	58										.....0..
CLV	B8										.0......
CMP		C9	CD	C5	D5	DD	D9	C1	D1		N.....ZC
CPX		E0	EC	E4							N.....ZC
CPY		C0	CC	C4							N.....ZC
DEC			CE	C6	D6	DE					N.....Z.
DEX	CA										N.....Z.
DEY	88										N.....Z.
EOR		49	4D	45	55	5D	59	41	51		N.....Z.
INC			EE	E6	F6	FE					N.....Z.
INX	E8										N.....Z.
INY	C8										N.....Z.
JMP			4C						6C[2]		....
JSR			20								....
LDA		A9	AD	A5	B5	BD	B9	A1	B1		N.....Z.
LDX		A2	AE	A6	B6[1]		BE				N.....Z.
LDY		A0	AC	A4	B4	BC					N.....Z.
LSR	4A		4E	46	56	5E					0.....ZC
NOP	EA										....
ORA		09	0D	05	15	1D	19	01	11		N.....Z.
PHA	48										....
PHP	08										....
PLA	68										N.....Z.
PLP	28										NV-BDIZC
ROL	2A		2E	26	36	3E					N.....ZC
ROR	6A		6E	66	76	7E					N.....ZC
RTI	40										NV-BDIZC
RTS	60										....
SBC		E9	ED	E5	F5	FD	F9	E1	F1		NV....ZC
SEC	38										1
SED	F8										....1...
SEI	78										.....1..
STA			8D	85	95	9D	99	81	91		....
STX			8E	86	96[1]						....
STY			8C	84	94						....
TAX	AA										N.....Z.
TAY	A8										N.....Z.
TSX	BA										N.....Z.
TXA	8A										N.....Z.
TXS	9A										....
TYA	98										N.....Z.

[1] Zero-Page,Y

[2] Indirekt, Drei-Byte-Befehl

Teamwork

INPUT 64-AssemblerSchule, Teil 6

Die einfachste Art, Maschinensprache-Programme zu starten, kennt sicherlich jeder von Ihnen: Der BASIC-Befehl SYS lädt die angegebene Adresse in den Programmzähler der CPU und führt so eine an dieser Stelle stehende Assembler-Routine aus. Damit kann man komplette Maschinenprogramme wie Spiele oder die Assembler-Schule starten. Will man aber kleine in Assembler geschriebene Hilfsroutinen einsetzen, ist in aller Regel eine Übergabe von Parametern an die Routine erforderlich. Auch die Ergebnisse dieser Routine sollen an das BASIC-Programm zurückgegeben werden.

Ging es bislang in diesem Kurs darum, die Befehle der 6502-CPU kennenzulernen und daraus Programme zusammenzusetzen, so werden wir uns in dieser abschließenden Folge darum kümmern, wie diese Programme benutzt werden können. Dabei geht es um Speicherbereiche, in denen Assemblerprogramme laufen können, aber auch um die Möglichkeiten der Parameterübergabe an Maschinensprache-Routinen und deren Zusammenarbeit mit BASIC-Programmen.

This is SYS

Dazu gibt es verschiedene Möglichkeiten. Sehen wir uns zunächst etwas genauer an, was der BASIC-Interpreter tut, wenn er einen SYS-Befehl abarbeitet. Bevor nämlich der Sprung in das Maschinensprache-Programm erfolgt, werden erst einmal die CPU-Register in einen definierten Zustand versetzt. Dazu dienen die Speicherstellen 780 bis 783 ($30C bis $30F). Mit deren Inhalt werden gemäß der Tabelle der Akku, die Index- und das Statusregister versorgt. Besonders die Adresse für das Status-Register ist hierbei mit Vorsicht zu genießen; eine gesetzte I- oder D-Flagge kann zu Problemen führen.

Für den eigentlichen Sprung in das Maschinenprogramm benutzt der BASIC-Interpreter einen JSR-Befehl. Dadurch kann man eine Maschinensprache-Routine mit dem RTS-Kommando abschließen und landet so wieder im BASIC-Programm, genau hinter dem SYS-Befehl. Vorher werden aber die Register wieder in die erwähnten Speicherstellen gerettet.

Man kann also mit dem BASIC-Befehl POKE vor dem Einsatz eines SYS-Kommandos die CPU-Register setzen. Hinterher können Sie sich mit PEEK ansehen, welchen Inhalt sie am Schluß der Routine hatten, und so Ergebnisse übergeben bekommen.

780 / $30C	Akkumulator
781 / $30D	X-Register
782 / $30E	Y-Register
783 / $30F	Prozessor-Status

Vier Speicherstellen dienen als Interface für den SYS-Befehl.

Braucht eine Routine mehr Parameter, als in den drei Registern Platz haben (das Statusregister ist ja nicht uneingeschränkt verwendbar), muß man noch andere Speicherzellen dazunehmen. Auf diese kann das Maschinenprogramm dann explizit zugreifen.

Übergabe programmiert . . .

Diese Art der Kommunikation zwischen Haupt- und Unterprogrammen ist zwar sehr einfach zu realisieren, aber relativ unkomfortabel zu bedienen. Das Unterprogramm in Maschinensprache ist schnell geschrieben. Aber durch die vielen POKE- und PEEK-Befehle wird das BASIC-Hauptprogramm sehr unübersichtlich und auch langsam.

Ein Beispiel soll dies verdeutlichen. Im Betriebssystem des C64 gibt es an der Adresse $FFF0 (65520) eine Routine, die den Cursor an eine bestimmte Bildschirmposition setzt. Mit ihr kann man etwas an einer definierten Stelle ausgeben. Diese Routine kann auch die derzeitige Cursor-Position als Ergebnis ermitteln — soll der Cursor gesetzt werden, so muß beim Eintritt in die Routine die Carry-Flagge gesetzt sein. Die Routine erwartet

die Zeile, in die der Cursor gesetzt werden soll, im X- und die Spalte im Y-Register. Nach dem bisher Gesagten kann man sie also mit folgender BASIC-Befehlsfolge aktivieren:

```
POKE 781,Z : REM Zeile in X
POKE 782,S : REM Spalte in Y
POKE 783,PEEK(783) AND 254 : REM Carry clear

SYS 65520 : REM Cursor setzen
PRINT "Text" : REM an Cursor-Position ausgeben
```

Selbst wenn man diese Befehlsfolge in eine BASIC-Zeile schreibt und die REMs wegläßt, ist sie doch relativ unübersichtlich.

Wünschenswert wäre etwa ein Aufruf der Art

SYS SC,Z,S : REM Cursor setzen
PRINT "Text" : REM an Cursor-Position ausgeben

wobei in SC die Startadresse einer Set-Cursor-Routine gespeichert ist und Z und S die Zeile beziehungsweise die Spalte enthalten. Diese Routine ist in Assembler einfach zu formulieren, da das Betriebssystem des C64 verschiedene Routinen zur Verfügung stellt, mit denen man Argumente direkt aus dem BASIC-Programmtext lesen kann. So gibt es ab Adresse $AEFD eine Routine, die überprüft, ob das nächste Zeichen ein Komma ist. Anderenfalls wird die Meldung 'SYNTAX ERROR' ausgegeben.

Die Routine, die an der Adresse $B7EB beginnt, ist für unseren Zweck wie geschaffen: Sie liest zwei durch Komma getrennte Zahlen aus dem Programmtext. Die erste darf dabei ein Zwei-Byte-Wert sein (wir brauchen nur das Low-Byte) und wird als Pointer in den Adressen $14 und $15 abgelegt. Die zweite muß ein Ein-Byte-Wert sein und wird im X-Register geliefert. Bei beiden Zahlen darf es sich übrigens auch um beliebige numerische Ausdrücke handeln.

Die zugehörige Maschinensprache-Routine haben wir als Listing abgedruckt. Sie ist nur 14 Bytes lang, bewirkt aber eine wesentlich komfortablere Erstellung von BASIC-Programmen, die den Cursor direkt adressieren sollen. Zudem arbeitet ein BASIC-Programm mit dieser Routine wesentlich schneller, als wenn man drei POKE- und einen SYS-Befehl einsetzt.

. . .und automatisch

Ein anderer Befehl zum Starten einer Maschinensprache-Routine, der leider sehr selten verwendet wird, ist die BASIC-Funktion USR(). Bei ihr wird die Startadresse des Assembler-Programms nicht explizit angegeben. Vielmehr gibt es an den Adressen $311 und $312 (785, 786) einen sogenannten USR-Vektor. Bei jedem Auftreten des USR-Befehles springt der Interpreter zu der in diesem Pointer angegebenen Adresse. Das Argument, das diese Funktion in Klammern übergeben bekommt, wird vorher ausgewertet und in einem speziellen Fließkommaformat in dafür vorgesehenen Adressen der Zero-Page abgelegt.

Diese Adressen sind für den BASIC-Interpreter reserviert und bilden den sogenannten Fließkomma-Akku (FAC). Er befindet sich an den Adressen $61 bis $66 und wird vom Interpreter für alle arithmetischen Funktionen benötigt, ähnlich dem Prozessor-Akkumulator, den die CPU ja in Assemblerprogrammen für Rechenoperationen benutzt.

Auch eine durch den USR-Befehl aktivierte Assembler-Routine kann mit RTS abgeschlossen werden. Damit nimmt der Interpreter seine Arbeit wieder an der Aufrufstelle im BASIC-Programm auf. Der USR-Befehl wird jedoch vom Interpreter wie eine Funktion — ähnlich wie SIN() oder EXP() — behandelt. Das heißt, er kann nicht wie der SYS-Befehl allein stehen, sondern liefert ein Ergebnis, das vom Programm weiterverarbeitet werden muß. Erlaubt sind zum Beispiel Konstruktionen wie

PRINT USR(x/10) oder
DU=USR(13)

Das Ergebnis der USR-Funktion wird vom Interpreter wieder im FAC erwartet. Falls Sie das Ergebnis nicht benötigen, können Sie die USR()-Funktion wie im zweiten Beispiel anwenden. Die Variable DU dient dann lediglich als Dummy.

Joystick-Akrobatik

Sie können aus Ihrem Programm heraus einen Quelltext für den INPUT-ASS (Ausgabe 6/86) abspeichern, der die Verwendung der USR-Funktion an einem Beispiel demonstriert. Der USR-Vektor wird dabei auf eine Routine gelenkt, die den Joystick abfragt. USR(1) liefert als Ergebnis 1, wenn der Stick nach rechts gedrückt ist, —1 bei einer Bewegung nach links und 0 wenn er sich in Mittelstellung befindet. Mit USR(2) kann die y-Richtung abgefragt werden, 1 bedeutet runter und —1 hoch. USR(3) ergibt 1, wenn der Feuerknopf gedrückt ist, sonst 0.

Das Programm beginnt mit einigen Bytes, die eine BASIC-Zeile darstellen. Jede BASIC-Zeile besteht aus einem Zeiger auf die nächste Zeile, der Zeilennummer in Low-High-Byte-Format und dem eigentlichen Text. Abgeschlossen wird sie durch ein Null-Byte. Das Programm liegt in sogenanntem Interpreter-Code vor, bei dem die BASIC-Schlüsselworte nicht als Klartext, sondern als Tokens (ein

```
01

c000            org $c000

c000 20fdae     jsr $aefd       Auf Komma pruefen
c003 20ebb7     jsr $b7eb       Zwei Zahlen holen
c006 8a         txa
c007 a8         tay             Spalte in Y
c008 a614       ldx $14         Zeile in X
c00a 18         clc
c00b 4cf0ff     jmp $fff0       Cursor setzen
```

Vierzehn Bytes reichen für eine komplette PRINT-AT-Routine.

Byte pro Wort) erscheinen. Der SYS-Befehl wird zum Beispiel als $9E verschlüsselt.

BASIC mal woanders

Durch die S-Anweisung wird sichergestellt, daß das eigentliche Programm auch wirklich an der in der BASIC-Zeile angegebenen Adresse beginnt. Dort wird zunächst der USR-Vektor „verbogen". Die folgenden Befehle dienen dazu, den BASIC-Anfang hochzusetzen. Mit dieser Formulierung ist folgendes gemeint: Normalerweise beginnt ein BASIC-Programm an der Adresse $801 (2049) im Speicher. Diese Adresse ist aber nicht fest, sondern wird durch den Inhalt der Speicherzellen $2B und $2C (43, 44) bestimmt. Sie enthalten einen Pointer auf das erste Byte des BASIC-Speichers.

Unser Beispielprogramm läßt sie auf das Label NEW, das letzte in diesem Programm, zeigen. Dadurch ist der Platz, den unsere USR-Routine belegt, vor Zugriffen durch den BASIC-Interpreter geschützt. Für ihn beginnt der Speicher praktisch erst an der Adresse NEW. Die beiden folgenden Betriebssystem-Aufrufe dienen dazu, auch andere interpreterspezifische Speicherstellen auf die neue Konfiguration einzustellen und ein eventuell an der Adresse NEW beginnendes BASIC-Programm zu starten.

So wie der Assembler das Programm auf Diskette schreibt, ist natürlich an dieser Stelle noch kein BASIC-Programm vorhanden. Wenn Sie aber das erzeugte Programm mit RUN starten, landen Sie wieder im BASIC-Direktmodus und können nun ein Programm eingeben oder laden, das die neuartige USR-Routine benutzt. Speichern Sie dieses Programm auf einen Datenträger, nachdem Sie mit der Befehlsfolge

POKE 43,1 : POKE 44,8

den BASIC-Anfang wieder auf den ursprünglichen Wert zurückgesetzt haben, dann wird beim erneuten Laden und Starten mit RUN zuerst wieder der USR-Vektor auf die Joystick-Routine gerichtet, und dann beginnt das BASIC-Programm zu arbeiten.

Ein Bit pro Richtung

Sehen wir uns nun die eigentliche Joystick-Abfrage an: Sie beginnt mit dem Aufruf einer Routine im BASIC-Interpreter, die die im FAC befindliche Fließkommazahl in einen Integer-Wert umrechnet. Sie liefert das High-Byte

Zum Programm

Die INPUT 64-Assembler-Schule setzt sich aus mehreren Teilen zusammen. Nach dem Laden sehen Sie ein Titelbild, von dem aus Sie mit einem beliebigen Tastendruck in das Hauptmenü gelangen.

Wenn Sie nun F1 drücken, gelangen Sie in ein Menü, das Ihnen verschiedene Themen zur Auswahl stellt. Die Erklärungen, die Sie jetzt abrufen können, sollten Sie parallel zum Beiheft lesen. Beide Medien ergänzen sich hier. Sie können die Erklärungen auch mit CTRL-B ausdrucken. Ins Hauptmenü gelangen Sie jederzeit mit der STOP-Taste zurück.

Mit F3 gelangen Sie aus dem Hauptmenü zu einer Auswahl verschiedener Beispielprogramme. Sie können eines davon auswählen, das Sie sich dann im Editor anschauen oder auch verändern können. Wenn Sie an dieser Stelle eine Null eingeben, enthält der Editor das zuletzt bearbeitete Programm, beim ersten Aufruf ist der Textspeicher leer.

Wenn Sie ein Beispielprogramm bearbeitet haben und — mit der STOP-Taste — wieder ins Hauptmenü springen, können Sie Ihren Text auch auf einen Drucker ausgeben lassen oder auf einen eigenen Datenträger abspeichern. Abgespeicherte Programme können Sie direkt mit dem INPUT-ASS (Ausgabe 6/86) laden und weiterbearbeiten.

Vom Editor aus gelangen Sie mit F7 in einen integrierten Simulator. Hier können Sie unsere Programmbeispiele oder Ihre selbstentworfenen Programme ablaufen lassen und testen, ob sie sich erwartungsgemäß verhalten.

Ausführliche Hinweise zur Bedienung des Editors und des Simulators sind im Programm enthalten. Sie können sie von dort aus jeweils mit der Funktionstaste F6 aufrufen. Es wird empfohlen, diese Seiten vor der Benutzung des Programmpakets einmal gründlich zu lesen. Besitzer eines Druckers können sie auch mit CTRL-B zu Papier bringen.

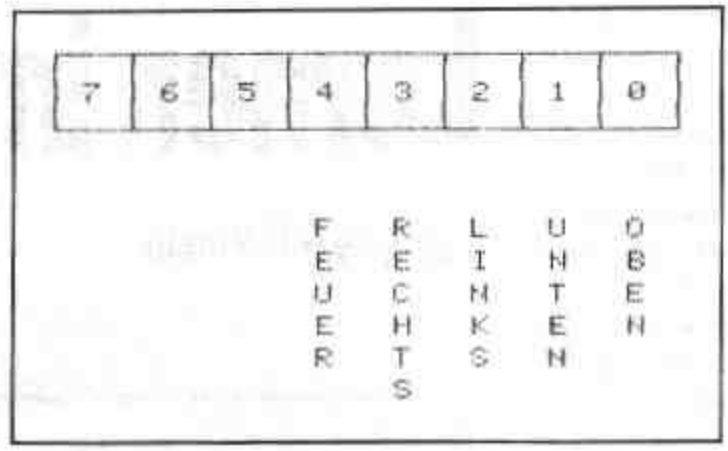
Die INPUT 64-Assembler-Schule ist eine Serie, die in Ausgabe 3/87 begonnen hat. Die einzelnen Lektionen bauen aufeinander auf. Wer noch keine Erfahrungen mit der Maschinensprache-Programmierung hat, tut gut daran, mit der ersten Folge anzufangen.

im Akku und das Low-Byte im Y-Register. Da unsere USR-Routine nur für die Argumente 1, 2 und 3 gedacht ist, muß das High-Byte gleich Null sein. Anderenfalls soll sie die Fehlermeldung „ILLEGAL QUANTITY ERROR" erzeugen.

Der SEI-Befehl, der nun folgt, verhindert für einige Zeit die Aktivierung der Tastaturabfrage in der Interrupt-Routine. Das ist notwendig, weil die Tastatur an den gleichen Ports der Peripherie-Chips (CIA, Complex Interface Adapter) hängt wie die Joystick-Stekker. Mit dem Zugriff auf das Datenrichtungsregister wird die CIA so programmiert, daß die für den Joystick zuständigen Bits (siehe Bild) als Eingang zur Verfügung stehen. Das Bitmuster landet im Akku. Anschließend wird die CIA in ihren Originalzustand versetzt und die Tastaturabfrage wieder zugelassen.

Im Y-Register steht immer noch die Zahl, mit der die USR-Routine aufgerufen wurde. Je nach ihrem Wert verzweigt das Programm nun zu verschiedenen Stellen, um die unterschiedlichen Richtungen abzufragen. Um diese Abfrage zu verstehen, müssen Sie noch wissen, daß das für den jeweiligen Joystick-Kontakt zuständige Bit Null wird, wenn der Kontakt geschlossen ist.

Das BASIC-Programm soll ja im FAC eine der Zahlen — 1, 0 oder 1 zurückbekommen. Um eine Zahl in den FAC zu bekommen, benutzen wir die Routine TOFAC ($BC44), die in der Zero-Page-Speicherzelle $62 das High-Byte und in $63 das Low-Byte einer Integerzahl erwartet. Ferner muß das X-Register $90 enthalten. Diese Routine endet mit einem RTS. Mit diesem Befehl landet der Prozessor wieder im Interpreter. Den Trick, direkt aufeinanderfolgende JSR- und RTS-Befehle durch ein JMP zu ersetzen, kennen Sie ja schon.



Das Datenregister A der CIAs ist zuständig für die Joystick-Anschlüsse.

Das zweite Source-File, das Sie sich aus dem Programm abspeichern können, enthält eine echte BASIC-Erweiterung. Mit diesem Programm wird es möglich, in BASIC-Programmen direkt Hexadezimalzahlen zu verwenden.

Hexerei

Diese Art der BASIC-Erweiterungen wird dadurch ermöglicht, daß der BASIC-Interpreter zwei Vektoren auf der Seite 3 benutzt. Immer wenn er im Programmtext ein Kommado (PRINT, POKE, RETURN etc.) erwartet, benutzt er den Befehl JMP ($308).

Normalerweise zeigt der Vektor $308/$309 auf die Adresse $A7E4. Dort beginnt eine Routine, mit deren Hilfe der Interpreter für jeden Befehl eine entsprechende Adresse findet, zu der er springt, um eben diesen Befehl zu behandeln. Ein zweiter wichtiger Vektor liegt auf den Adressen $30A/$30B. Dieser wird vom Interpreter immer dann verwendet, wenn er erkennt, daß ein auszuwertender Ausdruck folgt. Das kann eine Variable, ein Rechenausdruck oder ein String sein.

Genau diesen Vektor, der normalerweise auf die Adresse $AE86 zeigt, verwenden wir in unserem Beispiel. Er wird auf die Routine FUNCTION gerichtet. Die für das Verbiegen zuständigen Befehle sehen etwas umfangreich aus, sind aber aus folgenden Gründen notwendig:

Der Interpreter springt wie gesagt bei jedem Ausdruck über diesen Vektor. Wenn es sich dabei nun nicht um eine Hexadezimalzahl handelt, muß er ihn wie gewohnt behandeln, der ursprüngliche Inhalt des Vektors muß also gerettet werden. Dabei muß es sich nicht notwendigerweise um die Adresse $AE86 handeln, es kann ja vorher schon eine andere BASIC-Erweiterung geladen gewesen sein.

Die eigentliche Routine, auf die der Vektor für Ausdruckauswertung nun zeigt, beginnt mit einem Aufruf der Routine GETCHR. Mit dieser Routine liest der Interpreter Zeichen für Zeichen aus dem BASIC-Programmtext. Sie ist im Programm auf Ihrem Datenträger ausführlich erklärt.

Handelt es sich bei dem gelesenen Zeichen nicht um ein '$', so wird der Eingangszustand wiederhergestellt und zu der bei der Initialisierung geretteten Adresse gesprungen. Anderenfalls wird die Routine HEXIN aktiviert, die Sie anhand der Kommentare verstehen sollten. Die Umrechnung von Ziffern und Buchstaben in Hex-Werte ist die Umkehrung dessen, was Sie aus früheren Folgen unter dem Stichwort PBYT kennen.

Die Routine bricht ab, wenn ein Zeichen erkannt wird, das keine Hex-Ziffer darstellt. Zum Schluß wird das Ergebnis wieder mittels der Routine TOFAC in den Fließkomma-Akku übertragen. Daß die Adresse für TO-

FAC in diesem Programm eine andere als im ersten Beispiel ist, liegt daran, daß im ersten Beispiel auch ein negatives Ergebnis auftreten konnte. Hexadezimalzahlen sollen aber normalerweise nicht vorzeichenbehaftet sein. Wenn Sie wollen, daß diese Routine bei Zahlen größer als $7FFF ein negatives Ergebnis liefert, können Sie hier auch die Adresse aus dem ersten Beispiel einsetzen.

No Future?

An dieser Stelle endet unsere Assembler-Schule. Wir haben versucht, Ihnen die Grundlagen der Maschinensprache-Programmierung nahezubringen. Wenn Sie alle Folgen durchgearbeitet haben, sollten Sie in der Lage sein, zumindest Assemblerprogramme zu lesen und selbst kleinere Routinen in Maschinensprache zu entwickeln.

Natürlich kann eine sechsteilige Serie nicht alle Aspekte dieser Art und Weise, Programme zu entwickeln, behandeln. Aber bei Assemblerprogrammierung ist es wie bei allen Dingen, die man neu lernt: Übung macht den Meister und Probieren geht über Studieren.

Im übrigen werden Sie in INPUT 64 auch weiterhin Tips zur Assemblerprogrammierung und kommentierte Quelltexte finden. Sollten Sie einen Themenbereich vermißt haben, so schreiben Sie uns doch mal! Das Ende einer Serie ist noch lange kein Grund, keine weiteren Folgen zu bringen.

Hajo Schulz

Literatur

Christian Persson: 6502/65C02-Maschinensprache, Verlag Heinz Heise GmbH, Hannover 1983

Rodnay Zaks: Programmierung des 6502, Sybex-Verlag GmbH, Düsseldorf 1981