J. Ruppert

Läuft ein Programm einmal nicht so, wie es eigentlich soll, dann ist die Fehlersuche meistens ein mühsames "Geschäft" für den Hobby-Programmierer. Mit unserem Fehlersuchprogramm "6502-Tracer" wird der Inhalt der CPU-Register, des Stapels und des Stapelzeigers (Stack Pointer) bei jedem Programmschritt neben dem entsprechenden Befehl auf dem Bildschirm angezeigt.

6502-Tracer

Dem Programmfehler auf der Spur

Mit dem 6502-Tracer wollen wir nicht nur die glücklichen Besitzer eines Junior-Computers ansprechen, sondern auch die (nicht weniger glücklichen) Besitzer anderer 6502-Systeme. Das Programm belegt nur etwa ½ K Speicherbereich und braucht auf der Seite Null nicht mehr als 2 Byte. Mit wenigen Änderungen kann man es auch auf anderen 6502-Systemen zum Laufen bringen.

Wozu ist das gut?

Tatsächlich geht es darum, daß ein Programm schrittweise abgearbeitet und "sichtbar" gemacht wird, damit der Programmierer sein Programm in Ruhe analysieren, auf Fehler abklopfen und jedes Mal den Inhalt der Register A, X und Y sowie des Status- und des Stapel-Registers auf den Bildschirm holen kann. Bei der Aufzählung der Status-Flags (NV DIZC) fehlt das Break-Flag, weil unser Suchprogramm alle Befehle annimmt, außer denen, die zu einer Unterbrechung des Programms führen würden (BRK, IRQ und NMI).
Wie in Tabelle 3 zu sehen ist, kann ein Programmablauf (hier: eine Reihe von Befehlen, mit denen Register und Flags verändert werden) leicht analysiert werden, wenn man die Informationen der drei rechten Programmspalten zu nutzen weiß. Die Spalte ganz rechts betrifft den Stapel: FF ist das niederwertigste Byte des Zeigers (das höchstwertigste Byte ist Ø1). Am Ende der Liste finden sich einige Adressen, die beim Abarbeiten der Befehle JSR und RTS in den Stapel gebracht wurden. Die nächste Spalte gibt den logischen Pegel der Flags NV DIZC des Statusregisters an. Schließlich ist da noch der Inhalt der CPU-Register A, Y, X. Die Adressen und disassemblierten Befehle sind in den beiden Spalten ganz links aufgelistet und zeigen den Ablauf des Programms. Schritt für Schritt, Sprünge und Verzweigungen inbegriffen. Von der Adresse Ø2ØD (DØ FA) kommt man zur Adresse Ø2Ø9, wenn das Flag Z nicht logisch 1 ist.

Wie funktioniert's?

Leider können wir aus Platzmangel nicht das ganze Source-Listing des Suchprogramms abdrucken. Wir beschränken uns also auf eine Gebrauchsanleitung, einen Hexdump und eine kurze Beschreibung.
Bevor das Suchprogramm gestartet wird, muß die Startadresse des zu testenden Programms in die Speicherplätze ØØED und ØØEE geladen werden, deren Inhalt quasi die Funktion des Programmzählers übernimmt. Das getestete Programm kann in einem ROM gespeichert werden, das Suchprogramm muß aber in ein RAM: Die Startadresse lautet hier Ø5ØØ.
Mit den Adressen Ø5ØØ bis Ø523 wird eine Pufferzone von einigen Byte aufgebaut, die folgende Aufgaben übernimmt: Aufbau eines Pseudo-Stapels (ab Ø713 weiter unten), Ausgabe der Spaltenüberschriften und Setzen

Tabelle 1. 6502-TRACER ist ein Fehlersuch-Programm, das in ein RAM geladen werden muß. Wenn es dennoch in einem ROM abgelegt ist, muß es vor dem Abarbeiten erst in ein RAM übertragen werden.

Tabelle 1.

```
JUNIOR

M
HEXDUMP: 500,721
      Ø  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F
Ø5ØØ: 58 2Ø 95 Ø6 A9 ØØ A2 ØF 99 13 Ø7 88 DØ FA B9 CC
Ø51Ø: Ø6 2Ø A5 Ø6 C8 CØ 36 DØ F5 A9 26 8D 7E 1A A9 Ø5
Ø52Ø: 8D 7F 1A 4C A2 Ø5 8D 1B Ø7 68 8D 2Ø Ø7 68 68 8C
Ø53Ø: 1C Ø7 8E 1D Ø7 BA 8E 14 Ø7 D8 58 A2 Ø3 B9 15 Ø7
Ø54Ø: 2Ø A2 Ø6 2Ø A3 Ø6 C8 CØ Ø6 BØ 11 AD 16 Ø7 DØ Ø9
Ø55Ø: 2Ø A3 Ø6 2Ø A3 Ø6 4C 43 Ø5 CE 16 Ø7 CØ Ø9 DØ DD
Ø56Ø: AD 2Ø Ø7 29 CF 8D 13 Ø7 A2 Ø8 ØE 13 Ø7 9Ø Ø4 A9
Ø57Ø: 31 DØ Ø2 A9 2E 2Ø A5 Ø6 CA DØ EF 2Ø A3 Ø6 AD 14
Ø58Ø: Ø7 2Ø A2 Ø6 A9 2D 2Ø A5 Ø6 BA EØ FF BØ 14 68 8D
Ø59Ø: 16 Ø7 2Ø A2 Ø6 EØ FE BØ Ø5 68 48 2Ø A2 Ø6 AD 16
Ø5AØ: Ø7 48 A2 ØØ 2Ø 95 Ø6 A5 EE 2Ø A2 Ø6 A5 ED 2Ø A2
Ø5BØ: Ø6 2Ø A3 Ø6 B1 ED 8C 1A Ø6 8C 1B Ø6 8C 1A Ø7 8C
Ø5CØ: 19 Ø7 2Ø A8 Ø6 8C 1E Ø7 98 8D 16 Ø7 CE 16 Ø7 88
Ø5DØ: B1 ED 99 19 Ø6 99 18 Ø7 98 DØ F4 E6 ED DØ Ø2 E6
Ø5EØ: EE CE 1E Ø7 DØ F5 AD 18 Ø7 29 ØF DØ 13 AD 18 Ø7
Ø5FØ: C9 2Ø FØ 29 C9 4Ø FØ 2E C9 6Ø FØ 2E 29 1Ø DØ 62
Ø6ØØ: AD 18 Ø7 C9 4C FØ 2C C9 6C FØ 3D AE 1D Ø7 AC 1C
Ø61Ø: Ø7 AD 2Ø Ø7 48 AD 1B Ø7 28 DØ ØØ ØØ ØØ A5 ED 48
Ø62Ø: A5 EE 48 4C 33 Ø6 68 8D 2Ø Ø7 68 85 EE 68 85 ED
Ø63Ø: 4C 3D Ø6 AD 1A Ø6 85 ED AD 1B Ø6 85 EE A9 ØØ 8D
Ø64Ø: 19 Ø6 2Ø 9A Ø6 4C ØB Ø6 AD 1A Ø6 85 ED AD 1B Ø6
Ø65Ø: 85 EE A2 ØØ B1 ED AA C8 B1 ED 85 EE 8A 85 ED 4C
Ø66Ø: 3D Ø6 AD 2Ø Ø7 48 AD 18 Ø7 8D 6D Ø6 28 DØ Ø3 4C
Ø67Ø: 82 Ø6 58 D8 AD 1A Ø6 3Ø 11 18 65 ED 85 ED 9Ø Ø2
Ø68Ø: E6 EE A9 ØØ 8D 1A Ø6 4C ØØ Ø6 18 65 ED 85 ED BØ
Ø69Ø: F1 C6 EE 9Ø ED A9 ØD 2Ø A5 Ø6 A9 ØA 2Ø A5 Ø6 6Ø
Ø6AØ: 4C 8F 12 A9 2Ø 4C 34 13 AØ Ø1 C9 ØØ FØ 1A C9 4Ø
Ø6BØ: FØ 16 C9 6Ø FØ 12 AØ Ø3 C9 2Ø FØ ØC 29 1F C9 19
Ø6CØ: FØ Ø6 29 ØF AA BC Ø3 Ø7 8C 21 Ø7 6Ø 36 35 3Ø 32
Ø6DØ: 2Ø 2D 2Ø 54 52 41 43 45 52 ØD ØA 41 44 52 2E 2Ø
Ø6EØ: 2D 49 4E 53 54 52 2E 2D 2Ø 3A 41 2Ø 3A 59 2Ø 3A
Ø6FØ: 58 2Ø 4E 56 31 31 44 49 5A 43 2Ø 53 54 41 43 4B
Ø7ØØ: 2Ø ØD ØA Ø2 Ø2 Ø2 Ø1 Ø2 Ø2 Ø2 Ø1 Ø1 Ø2 Ø1 Ø1 Ø3
Ø71Ø: Ø3 Ø3 Ø3 8Ø FB ØØ ØØ ØØ DØ FD ØØ Ø4 71 Ø8 ØØ ØØ
Ø72Ø: 31 Ø2

JUNIOR
```

des Vektors IRQ (das Unterprogramm IRQ beginnt bei Adresse Ø526).
Ab Adresse Ø5A2 beginnt das eigentliche Suchprogramm: Anzeigen der Programmzähler-Adressen, Laden der Op-Kodes, Auffüllen des Arbeitsspeicherbereichs mit ØØ, Berechnen der Befehlslänge (das dazu notwendige Unterprogramm fängt bei Ø6A8 an und ähnelt dem Unterprogramm LENACC des Junior). Der Arbeitsspeicher ist ein Bereich von 4 Byte RAM (Ø619 . . . Ø61C), in den das Suchprogramm nach und nach alle Befehle des zu testenden Programms einschreibt, um sie dann auszuführen. Da diese Befehle nie mehr als 3 Byte haben, folgt immer mindestens einmal ØØ, und das wirkt wie ein BRK-Befehl. Also wird das zu testende Programm, gleich nachdem ein Befehl ausgeführt worden ist, unterbrochen und das Unterprogramm IRQ (ab Ø526) gestartet.
In Ø5DB wird eine Art Programmzähler erzeugt (ØØED . . . ØØEE), der vom Format des vorhergehenden Befehls abhängt; dessen Länge wiederum ist in Adresse Ø71E gespeichert. Ab Adresse Ø5E6 werden alle Sprungbefehle herausgenommen und später, wenn nötig, abgearbeitet. Ab Ø6ØB werden die Register A, X und Y des zu testenden Programms im Stapel abgelegt.
Weiter geht es mit Adresse Ø619, dem Arbeitsspeicherbereich, der jetzt den Befehl vom getesteten Programm enthält. Danach kommen wieder ein BRK-Befehl und das Unterprogramm IRQ. Man braucht sich nicht zu wundern, daß dieses Programm die Prozessorregister, so wie sie nach dem Ausführen des eben erwähnten Programmbefehls sind, im Stapel ablegt – das ist normal. Schließlich wird der ganze Registerinhalt festgehalten und der nächste Befehl ausgeführt.
In Adresse Ø61D befinden sich spezielle Unterprogramme für die Bearbeitung von Sprungbefehlen. Relative Sprünge werden in Ø672 und Ø68A berechnet. Die Adressen Ø6A1, Ø6A2 und 06A6, Ø6A7 enthalten die Adressen der Unterprogramme PRBYT und PRCHA des Junior-Computers, die geändert werden müssen, wenn man ein anderes 6502-System verwenden will.
Von Ø6CC bis Ø7Ø2 sind die Druckanweisungen für die Spaltenüberschriften gespeichert; Ø7Ø3 bis Ø712 enthalten die Lookup-Tabelle des Unterprogramms, mit dem das Format der auszuführenden Befehle festgelegt wird. Die Adressen Ø713 bis Ø721 beinhalten noch ein paar Pufferbytes, die unser Suchprogramm braucht, um den Stapelzeiger, den Inhalt der "Stapelspitze", den Operationskode (der in diesem Moment verwendet wird), die Länge des dazugehörigen Befehls, den Programmzähler usw. zu speichern.
Wir hoffen, daß die Fehlersuche in einem Programm in Zukunft zu einem Kinderspiel wird.

Tabelle 2.

```
JUNIOR

M
HEXDUMP: 200,23A
      Ø  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F
Ø200: A9 Ø3 A8 AA A9 Ø9 85 ØØ F8 18 65 ØØ CA DØ FA 2A
Ø210: 6A 38 E5 ØØ 88 DØ FA E5 ØØ D8 FØ ØØ FØ Ø6 FØ Ø2
Ø220: FØ Ø4 FØ FC FØ F8 2Ø 3Ø Ø2 38 EA 4C 35 Ø2 EA EA
Ø230: 2Ø 34 Ø2 6Ø 6Ø 4C ØØ Ø3 4C ØØ Ø2

JUNIOR

M
HEXDUMP: 2FØ,3ØF
      Ø  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F
Ø2FØ: ØØ ØØ ØØ ØØ ØØ ØØ ØØ ØØ ØØ ØØ ØØ ØØ B0 Ø6 B0 Ø2
Ø3ØØ: B0 FC B0 F8 6C Ø7 Ø3 ØØ Ø2 ØØ ØØ ØØ ØØ ØØ ØØ ØØ
Ø31Ø:
```

Tabelle 3.

```
ED
ØØED 27 ØØ.
ØØEE Ø9 Ø2.
ØØEF 1C 5ØØ
Ø5ØØ 58 R
6502 - TRACER
ADR. -INSTR.- :A :Y :X NV1BDIZC STACK
Ø2ØØ A9 Ø3     Ø3 ØØ ØØ ........ FF-
Ø2Ø2 A8        Ø3 Ø3 ØØ ........ FF-
Ø2Ø3 AA        Ø3 Ø3 Ø3 ........ FF-
Ø2Ø4 A9 Ø9     Ø9 Ø3 Ø3 ........ FF-
Ø2Ø6 85 ØØ     Ø9 Ø3 Ø3 ........ FF-
Ø2Ø8 F8        Ø9 Ø3 Ø3 ....1... FF-
Ø2Ø9 18        Ø9 Ø3 Ø3 ....1... FF-
Ø2ØA 65 ØØ     18 Ø3 Ø3 ....1... FF-
Ø2ØC CA        18 Ø3 Ø2 ....1... FF-
Ø2ØD DØ FA     18 Ø3 Ø2 ....1... FF-
Ø2Ø9 18        18 Ø3 Ø2 ....1... FF-
Ø2ØA 65 ØØ     27 Ø3 Ø2 ....1... FF-
Ø2ØC CA        27 Ø3 Ø1 ....1... FF-
Ø2ØD DØ FA     27 Ø3 Ø1 ....1... FF-
Ø2Ø9 18        27 Ø3 Ø1 ....1... FF-
Ø2ØA 65 ØØ     36 Ø3 Ø1 ....1... FF-
Ø2ØC CA        36 Ø3 ØØ ....1.1. FF-
Ø2ØD DØ FA     36 Ø3 ØØ ....1.1. FF-
Ø2ØF 2A        6C Ø3 ØØ ....1... FF-
Ø21Ø 6A        36 Ø3 ØØ ....1... FF-
Ø211 38        36 Ø3 ØØ ....1..1 FF-
Ø212 E5 ØØ     27 Ø3 ØØ ....1..1 FF-
Ø214 88        27 Ø2 ØØ ....1..1 FF-
Ø215 DØ FA     27 Ø2 ØØ ....1..1 FF-
Ø211 38        27 Ø2 ØØ ....1..1 FF-
Ø212 E5 ØØ     18 Ø2 ØØ ....1..1 FF-
Ø214 88        18 Ø1 ØØ ....1..1 FF-
Ø215 DØ FA     18 Ø1 ØØ ....1..1 FF-
Ø211 38        18 Ø1 ØØ ....1..1 FF-
Ø212 E5 ØØ     Ø9 Ø1 ØØ ....1..1 FF-
Ø214 88        Ø9 ØØ ØØ ....1.11 FF-
Ø215 DØ FA     Ø9 ØØ ØØ ....1.11 FF-
Ø217 E5 ØØ     ØØ ØØ ØØ ....1.11 FF-
Ø219 D8        ØØ ØØ ØØ ......11 FF-
Ø21A FØ ØØ     ØØ ØØ ØØ ......11 FF-
Ø21C FØ Ø6     ØØ ØØ ØØ ......11 FF-
Ø224 FØ F8     ØØ ØØ ØØ ......11 FF-
Ø21E FØ Ø2     ØØ ØØ ØØ ......11 FF-
Ø222 FØ FC     ØØ ØØ ØØ ......11 FF-
Ø22Ø FØ Ø4     ØØ ØØ ØØ ......11 FF-
Ø226
     2Ø 3Ø Ø2 ØØ ØØ ØØ ......11 FD-Ø229
Ø23Ø
     2Ø 34 Ø2 ØØ ØØ ØØ ......11 FB-Ø233
Ø234
     6Ø        ØØ ØØ ØØ ......11 FD-Ø229
Ø233
     6Ø        ØØ ØØ ØØ ......11 FF-
Ø229 38        ØØ ØØ ØØ ......11 FF-
Ø22A EA        ØØ ØØ ØØ ......11 FF-
Ø22B
     4C 35 Ø2 ØØ ØØ ØØ ......11 FF-
Ø235
     4C ØØ Ø3 ØØ ØØ ØØ ......11 FF-
Ø3ØØ B0 FC     ØØ ØØ ØØ ......11 FF-
Ø2FE B0 Ø2     ØØ ØØ ØØ ......11 FF-
Ø3Ø2 B0 F8     ØØ ØØ ØØ ......11 FF-
Ø2FC B0 Ø6     ØØ ØØ ØØ ......11 FF-
Ø3Ø4
     6C Ø7 Ø3 ØØ ØØ ØØ ......11 FF-
Ø2ØØ A9 Ø3     Ø3 ØØ ØØ .......1 FF-
Ø2Ø2 A8        Ø3 Ø3 ØØ .......1 FF-
Ø2Ø3 AA
JUNIOR
```

Tabelle 2. Man kann diese Befehle benutzen, um das Programm aus Tabelle 1 zu testen. Herauskommen sollte dann, was in Tabelle 3 zu sehen ist.

Tabelle 3. Dies erscheint auf dem Bildschirm (oder wird ausgedruckt), wenn das Programm aus Tabelle 2 mit Hilfe des Suchprogramms ausgeführt wird. Vor dem Start von 6502-Tracer in Ø5ØØ wird erst die Startadresse des zu testenden Programms (Ø2ØØ) auf Seite Null (ØØED und ØØEE) "geschrieben".