6502 Disassembler#

by von Georg Rehfeldt, Vierte Dimension 1/1985

(translation pending)

see also 6502 DISASSEMBLER

Ein Disassembler für den 6502#

In Ergänzung zu einem Decompiler benötigt man oft eine Möglichkeit, Maschinencode listen zu können. Damit kann man sich ein Bild von den Kernal-Routinen und anderen Code-Definitionen machen. Häufig verfügt der Computer über einen elngebauten oder zuladbaren Maschinensprache-Monitor, der einen Disassembler enthält. Für alle FORTH-Freunde, die mit einem 6502-System arbeiten und keinen Disassernbier besitzen, der von FORTH aus ansprechbar ist, folgt hier ein Disassembler, der vollständig in FORTH formuliert ist. Er läßt sich relativ einfach in den vorgenannten Decompiler einbinden.

Untersucht man die Opcodes des 6502 anhand einer hexadezimal sortierten Befehlsliste, so fällt sofort auf, daß alle Befehle, deren niederwertiges Bit Nr. 0 gesetzt ist, eine große Reglmäßigkeit aufweisen. Diese Hälfte der Opcodes kann man einfach weiter unterteilen: alle Opcodes, deren Bit Nr. 1 ebenfalls gesetzt ist, ($03, $07, $0B, $0F, $13,...) sind keine gültigen Befehle. Das andere Viertel der Opcodes mit gesetztem Bit Nr. 0 und nicht gesetztem Bit Nr. 1 ($01, $05, $09, $0D,...) sind die 8 Befehle: ORA, AND, EOR, ADC, STA, LDA, CMP und SBC mit je 8 Adressierungsarten (ind,X), Zero-Page, immediate, absolut, (ind),Y , Zero Page,X, absolut,Y und absolut,X. Es gibt nur die eine logische Ausnahme: einen Befehl STA ZZ gibt es nicht.

Bei der anderen Hälfte der Opcodes mit nicht gesetztem Bit Nr. 0 läßt sich eine Regelmäßigkeit nicht so einfach feststellen. Der folgende Disassembler faßt deshalb diese Hälfte der Opcodes in der Tabelle SHORTCODE mit ihren wesentlichen Daten zusammen. Die Daten der sytematischen Hälfte der Opcodes sind in die beiden kurzen Tabellen SCODE und ADRMODE gefaßt, die von dem Wort SHORTCODE1 ausgewertet werden. Das Wort SHORTCODE0 schließlich liefert die für alle Opcodes benötigten Informationen.

Das Wort DIS schließlich disassembliert ab der Adresse, die auf dem Stack liegt, Zelle für Zeile, bis das Disassembling mit RETURN abgebrochen wird. Es benutzt dazu außer SHORTCODE einige Tabellen mit ASCII-Zeichen. Noch eine Bemerkunq zur Art und Weise, wie das Wort TABELLE die Zahlen einliest: Die Ubergabe der Zahlen auf dem Stack ist in FIG-6502-Systemen wegen der bedauerlich kleinen Stacktiefe nicht möglich, deshalb der mühsame Weg über BL WORD HERE NUMBER DROP.