

A Decompiler for FIG-Forth#

Vierte Dimension 1/1985

by Georg Rehfeldt

(translation pending)

Wie sicherlich die meisten von Euch wissen, erzeugt der FORTH-Compiler beim Schreiben von neuen Wortdefinitionen (z.B. : 2DUP OVER OVER ;) ins Wörterbuch zunächst einen Kopf, der außer dem Namen des Wortes (2DUP) und seiner Länge (4) noch andere Angaben enthält. Zunächst gibt es einen Zeiger auf ein vorhergehend kompiliertes Wort; dieser Zeiger wird zum Durchsuchen des Wörterbuchs verwandt. Dann existiert noch ein Zeiger auf ausführbaren Maschinencode, der vom inneren Interpreter benötigt wird. Die Adresse dieses Zeigers heißt Compilationsadresse des Wortes (CFA in FIG-FORTH). Außer dem Kopf wird in der Regel noch ein Rumpf ins Wörterbuch geschrieben. Bei einer Colon-Definition, ein Wort, das mit ":" eingeleitet und in der Regei mit ";" abgeschlossen wird, werden die Compilationsadressen der nach dem Namen folgenden Worte (OVER OVER) im Wörterbuch nacheinander abgelegt. Eine ":"-Definition besteht also aus dem Kopf und einer Liste von Compilationsadressen, die den Rumpf bildet. Der innere Interpreter von FORTH kann aus diesen Zeigern bei der Ausführung des Wortes "2DUP " die Worte "OVER OVER" wiedererkennen, denn jedes FORTH-Wort ist durch seine Compilationsadresse eindeutig gekennzeichnet.

Diese Tatsache macht sich der hier gezeigte Decompiler zunutze. Er ist in der Lage, compilierte Worte wieder lesbar auszulisten. Dies ist zur Fehlersuche in eigenen Worten ganz nützlich, eignet sich jedoch auch zur Analyse schlecht dokumentierter FORTH Versionen und hilft nicht zuletzt dem Anfänger beim Verständnis des Compilationsprozesses in FORTH.

Nicht alle FORTH-Worte compilieren einfach durch Ablage Ihrer Compilationsadresse im Wörterbuch, es gibt zum Beispiel die IMMEDIATE-Worte, in der Regel Anweisungen an den Compiler, die etwas anderes ins Worterbuch schreiben als ihre eigene Compilationsadresse. (So compiliert IF ein OBRANCH, ELSE ein BRANCH, jeweils mit nachfolgender, relativer Sprungadresse und THEN überhaupt nichts ins Wörterbuch.) Eine ausführliche Beschreibung aller Sonderfälle führt hier zu weit, das Decompilieren selbstformulierter Worte zeigt das Verhalten dieser besonderen Worte am besten.

Die Bedienung des Decompilers ist einfach, einzutippen ist z.B.:

```
DEC 2DUP      (RETURNTASTE)
```

und der Decompiler antwortet mit :

```
2DUP CFA 1234 INH 5678
1236 OVER
1238 OVER
123A ;S
```

Es gibt einige Worte, die nicht mit ;S oder (;CODE) enden, wie ABORT und QUIT, weil das Ende dieser Worte niemals erreicht wird. Bei diesen Worten kann der Decompiler das Ende des Wortes nicht erkennen und das Listing muß, wie beim vorzeitig gewünschten Abbruch, mit ?TERMINAL beendet werden.

Ein automatischer Decompiler hat einen großen Nachteil: Bei Erweiterungen des Compilers wie z.B. durch selbstdefinierte Definitionsworte, müßte der Decompiler entsprechend erweitert werden. Dies muß der Anwender jedoch selbst tun, oder die mit den grundlegenden Worten aus Screen Nr. 13

geschaffenen einfachen interaktiven Worte in Screen Nr. 17 benutzen, um solche Besonderheiten zu decompilieren.