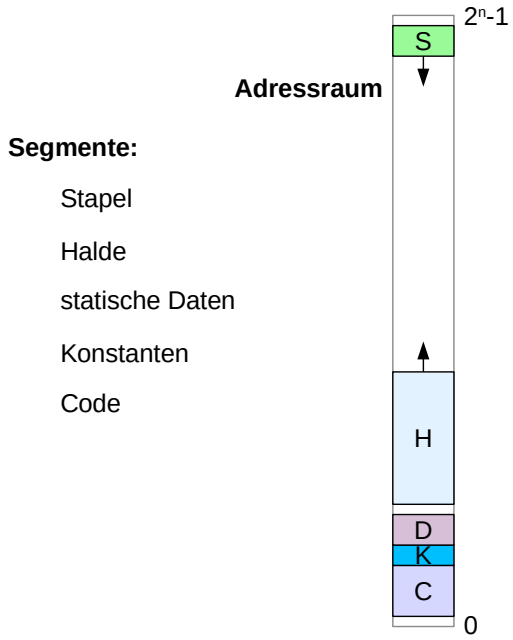
Segmente und Adressräume

DHBW Stuttgart

Roland Weber

Im Begleitbuch:
- Teile von Kapitel 3 “Software”
- Einstieg in Kapitel 13 “Adressen”

Programm im Speicher

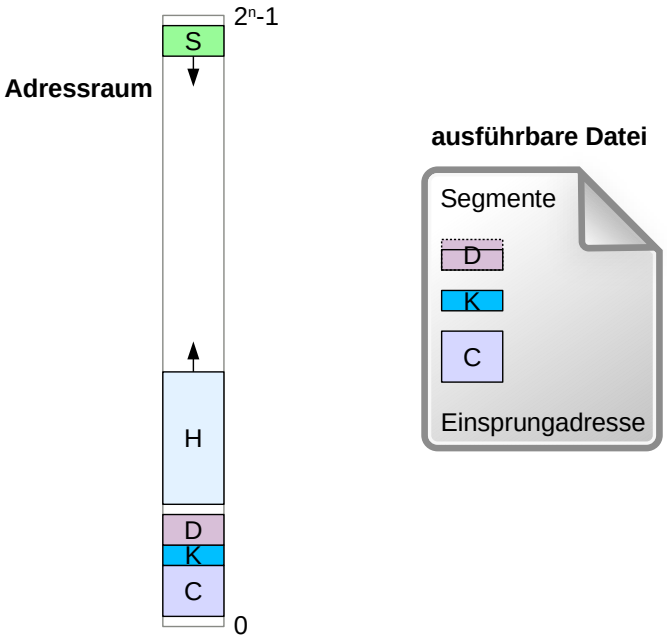


Eine Instanz ist ein laufendes Programm. Der “Lebensraum” der Instanz ist ihr Adressraum. Dort laufen ihre Befehlsströme ab und greifen über Adressen auf den Hauptspeicher (RAM) zu. Die Instanz darf aber nur bestimmte Bereiche des Speichers bzw. ihres Adressraums benutzen.

Eine Instanz verwendet zusammenhängende Bereiche im Adressraum, genannt Segmente. Hier sind stellvertretend 5 davon dargestellt, es gibt mehr.

Code: ausführbar, nur lesbar
Konstanten: Daten, nur lesbar
statische Daten: Daten, schreibbar, Größe statisch
Halde: Daten, schreibbar, dynamisch angefordert
Stapel: Daten, schreibbar, für lokale Variablen

Programm in Datei

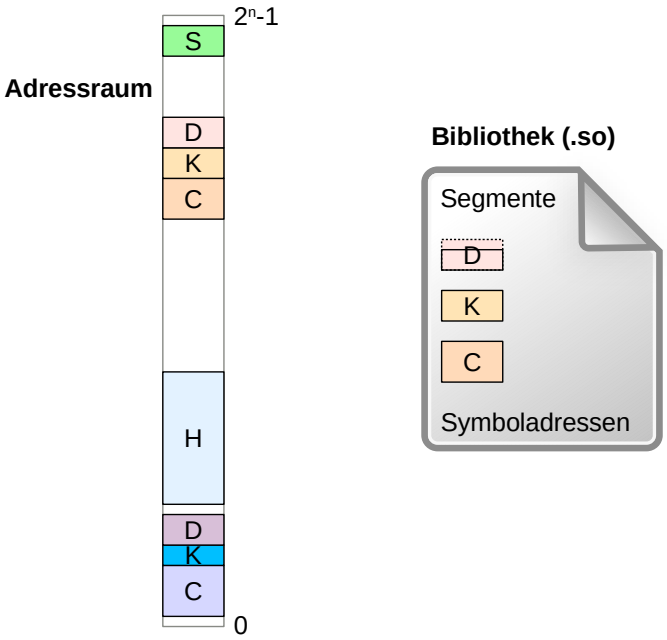


Segmente fester Größe werden von Compiler und Linker in einer ausführbaren Datei definiert. Bei statischen Daten spart man Platz, indem man nicht- oder 0-initialisierte Daten in der Datei weglässt.

Die Ausführung eines Programms muss irgendwo im Code starten. Die Einsprungadresse steht in der ausführbaren Datei.

Halde und Stapel werden beim Programmstart angelegt. Die Halde ist leer. Auf dem Stapel übergibt der Programmlader Aufrufargumente des Programms und Umgebungsvariablen. Diese Informationen sind beim Erstellen der ausführbaren Datei nicht bekannt.

Dynamische Bibliothek

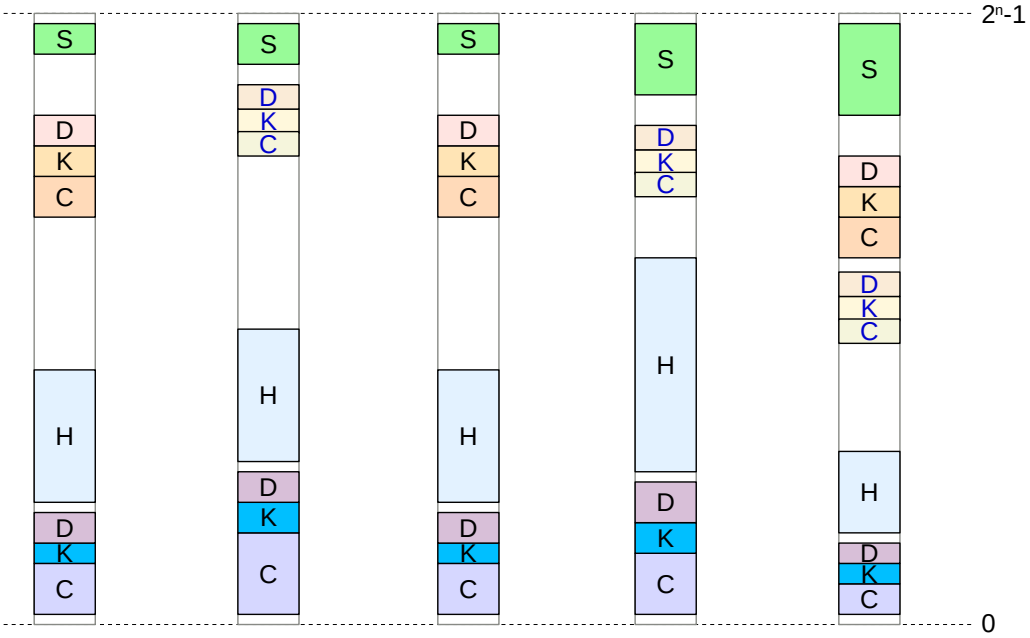


Dynamische Bibliotheken sind eigene Dateien, die zusätzlich zum Programm in den Adressraum geladen werden müssen. Compiler und Linker definieren wiederum Segmente fester Größe, wie bei einer ausführbaren Datei.

Bibliotheken werden nicht ausgeführt, sondern aufgerufen. Deshalb keine Einsprungadresse, sondern eine Tabelle mit Adressen von Symbolen, vor allem Funktionen.

Der Code des Programms enthält Funktionsaufrufe mit Symbolen als Ziel. Der Programmlader biegt diese Aufrufe auf die Adressen der geladenen Bibliothek um.

Mehrere Adressräume



In jedem Adressraum stehen die gleichen Adressen zur Verfügung. Was an einer Adresse liegt hängt davon ab, was in den jeweiligen Adressraum geladen wurde.

Adressen gelten nur innerhalb eines bestimmten Adressraums. Wie Telefonnummern ohne Vorwahl.

Eine dynamische Bibliothek liegt in verschiedenen Adressräumen an unterschiedlichen Adressen. Der Compiler übersetzt sie in “position independent code” (PIC) damit das funktioniert.

Ausführbare Dateien werden für gewöhnlich ebenfalls in PIC übersetzt. Das ist eine Voraussetzung für “address space layout randomization” (ASLR).