

64-041 Übung Rechnerstrukturen und Betriebssysteme



Aufgabenblatt 1 Ausgabe: 15.10., Abgabe 22.10.2025 24:00

Gruppe	
Name(n)	Matrikelnummer(n)

Aufgabe 1.1 (Punkte 10+10+10+10+10)

Horner-Schema: Durch nachlässige Programmierung kann die Leistung eines Computersystems oft erheblich beeinträchtigt werden. Nehmen wir an, die CPU (Central Processing Unit) unseres Rechners verfügt über Befehle zur Multiplikation und zur Addition von Zahlen, und sie kann eine Multiplikation in 5 ns und eine Addition/Subtraktion in 1 ns ausführen.

In dieser Aufgabe betrachten wir als Beispiel die Auswertung von Polynomen.

- (a) Wie lange dauert auf dieser CPU die Auswertung eines Polynoms sechsten Grades direkt nach der üblichen Formel $z = (a \cdot x^6 + b \cdot x^5 + c \cdot x^4 + d \cdot x^3 + e \cdot x^2 + f \cdot x + g)$?
- (b) Wie lange benötigt die CPU dagegen, wenn das Polynom nach dem Horner-Schema berechnet wird? — ggf. im Mathe-Skript/WWW/Wikipedia (<https://de.wikipedia.org/wiki/Horner-Schema>) nachlesen. Geben Sie auch die im Beispiel notwendigen Rechenschritte an.
- (c) Polynome höheren Grades kommen allerdings in Anwendungen nur selten vor. Häufiger sind Polynome ersten und zweiten Grades von mehreren Variablen, hier x und y . Dabei treten auch gemischte Terme auf: $z = (a \cdot x^2 + b \cdot y^2 + c \cdot xy + d \cdot x + e \cdot y + f)$. Wie lange dauert die naive Berechnung in diesem Fall?
- (d) Ist in diesem Fall (c) ein Horner-Schema überhaupt möglich? Begründen Sie, und geben Sie die Berechnungsschritte und die Ausführungszeit an:
- (e) Überlegen Sie sich die optimale Auswertung von:
 $z = (a \cdot x^3 + b \cdot y^3 + c \cdot x^2y + d \cdot xy^2 + e \cdot x^2 + f \cdot y^2 + g \cdot xy + h \cdot x + i \cdot y + j)$:

Aufgabe 1.2 (Punkte 20)

Hohe Potenzen: Bei bestimmten Kryptoalgorithmen (z.B. Diffie-Hellmann) müssen hohe Potenzen eines Ausdrucks berechnet werden.

- (a) Der Ausdruck $y = (x^2 - 6 \cdot x + 9)^{17}$ soll mit den Operationen Addition und Multiplikation möglichst effizient berechnet werden. Dazu können Sie die Variablen a, b, \dots für Zwischenergebnisse verwenden.

Wie viele Rechenoperationen werden minimal benötigt und welche Ausführungszeit ergibt sich für die Berechnung des Ausdrucks?

Aufgabe 1.3

10+20 *Selbstmodifizierender Code*: Beim von-Neumann Konzept werden sowohl Programme als auch Daten gemeinsam im Speicher des Computers abgelegt. Programme können daher prinzipiell genauso wie Daten durch den Prozessor verändert werden und sich sogar selbst modifizieren. Dies galt anfangs als großer Vorteil, wird mittlerweile aber nur noch in Ausnahmefällen verwendet, weil es die Fehlersuche massiv erschwert.

- (a) Wie kann ein Computervirus/Schadprogramm von einer Webseite zunächst als harmloser Download (Daten) in den Rechner gelangen, dann aber als Programm ausgeführt werden?
- (b) Die Java Hotspot Virtuelle Maschine benutzt ein mixed mode Ausführungsmodell: nur die besonders häufig aufgerufenen Funktionen eines Programms werden erst zur Laufzeit aufwendig kompiliert und optimiert, selten benutzte Funktionen aber interpretiert. Nennen Sie einige Vor- und Nachteile dieses Konzepts.