Kapitel 1

Einleitung

Wir geben einige Beispiele für effiziente Algorithmen, die wir zum Teil später wieder aufgreifen und vertiefen werden. Zunächst geht es nur darum, einen ersten Einblick in die behandelten Probleme und verwendeten Methoden zu geben.

1.1 Schnelle Multiplikation von Zahlen

Seien x, y Zahlen in endlich b-adischer Darstellung, $b > 1$, also

$$\begin{array}{rcl} x &=& x_0 + x_1 b + \ldots + x_{n-1} b^{n-1} \quad , \quad 0 \leq x_i < b \, , \\ y &=& y_0 + y_1 b + \ldots + y_{n-1} b^{n-1} \quad , \quad 0 \leq y_i < b \end{array}$$

mit ganzen Zahlen x_i, y_i. Gesucht ist das Produkt $z = xy$. Die Schulmethode soll an Hand eines Beispiels mit $b = 10$ und $n = 3$ erläutert werden:

$$\begin{array}{r} \underline{214 \cdot 713} \\ 642 \\ 214 \\ \underline{1498} \\ 152582 \end{array}$$

Offenbar benötigt die Schulmethode für eine Multiplikation der Länge n $\mathrm{O}(n^2)$ Rechenoperationen. Addiert man, sobald in einer Spalte alle Produkte berechnet sind, so kommt man mit $\mathrm{O}(n)$ Speicherplätzen aus.

Der Schulmethode stellen wir als effizienten Algorithmus die Karatsuba-Multiplikation gegenüber. Sei n gerade und $n = 2m$. Wir teilen x auf in

$$\xi_0 = x_0 + x_1 b + \ldots + x_{m-1} b^{m-1} \ , \quad \xi_1 = x_m + x_{m+1} b + \ldots + x_{n-1} b^{m-1}$$

und entsprechend $y = \eta_0 + b^m \eta_1$. Dann ist

$$\begin{aligned} xy &= \xi_0\eta_0 + (\xi_0\eta_1 + \xi_1\eta_0)b^m + \xi_1\eta_1 b^n \\ &= (1 + b^m)\xi_0\eta - b^m(\xi_1 - \xi_0)(\eta_1 - \eta_0) + (b^m + b^n)\xi_1\eta_1 \ . \end{aligned}$$

Wir können also eine Multiplikation der Länge n realisieren durch 3 Multiplikationen der Länge $n/2$ sowie $\mathrm{O}(n)$ zusätzliche Rechenoperationen. Ist also $T(n)$ die Anzahl der Rechenoperationen, die wir für eine Multiplikation der Länge n benötigen, so gilt

$$T(n) \leq 3T(\frac{n}{2}) + cn \quad , \quad T(1) = 1$$

mit einer von n unabhängigen Konstanten c. Ist nun n eine Zweierpotenz, also $n = 2^p$, so ist mit $T_p = T(2^p)$

$$T_p \leq 3T_{p-1} + c2^p \ , \quad T_0 = 1 \ . \tag{1.1.1}$$

Lemma 1.1.1 *Seien T_p, q, $r_p \geq 0$, und sei*

$$T_{p+1} \leq qT_p + r_p \ , \quad p = 0, 1, \ldots \ .$$

Dann ist

$$T_p \leq q^p T_0 + \sum_{j=0}^{p-1} q^{p-1-j} r_j \ .$$

Der Beweis durch vollständige Induktion ist trivial.

Satz 1.1.2 *Für $n = 2^p$ kann die Multiplikation der Länge n in $O(n^{\log_2 3})$ Rechenoperationen durchgeführt werden.*

Beweis: Wenden wir Lemma 1.1.1 auf (1.1.1) an, so entsteht

$$\begin{aligned} T_p &\leq 3^p + c\sum_{j=0}^{p-1} 3^{p-1-j}2^{j+1} \\ &= 3^p + c3^p \sum_{j=0}^{p-1} \left(\frac{2}{3}\right)^{j+1} \\ &\leq 3^p + c3^p \, \frac{2}{3} \, \frac{1}{1-2/3} = (1+2c)3^p \\ &= (1+2c)n^{\log_2 3} \, . \end{aligned}$$

□

Wegen $\log_2 3 = 1.585 < 2$ ist dies eine Verbesserung gegenüber der $O(n^2)$-Abschätzung für die Schulmethode, jedenfalls für große n. Das Karatsuba-Verfahren kann leicht durch ein rekursives Programm realisiert werden:

```
fmult (n, x, y, z)

{ if    (n == 1) Schulmethode;
  else
  {     m = n/2;
        ξ0 = (x0, ..., x(m-1)); ξ1 = (xn, ..., x(n-1));
        η0 = (y0, ..., y(m-1)); η1 = (ym, ..., y(n-1));
        fmult (m, ξ0, η0, α);
        fmult (m, ξ1 - ξ0, η1 - η0, β);
        fmult (m, ξ1, η1, γ) for (i = 0; i < n; i++) zi = 0;
        for (i = 0; i < n; i++)
          { zi = αi + zi;
            z(i+m) = αi - βi + γi + z(i+m);
            z(i+n) = γi + z(i+n);
          }
  }
}
```

Der Karatsuba-Algorithmus ist ein typisches Beispiel für die oft verwendete “Divide-and-Conquer-Statgie”: Ein Problem wird in kleinere Teilprobleme zerlegt. Diese werden gelöst und aus den Lösungen die Lösung des ursprünglichen Problems zusammengesetzt. Dieser Prozeß wird in rekursiver Weise wiederholt.

1.2 Schnelle Multiplikation und Inversion von Matrizen

Zur Multiplikation zweier (n,n)-Matrizen A, B nach der Schulmethode benötigt man bekanntlich $\mathrm{O}(n^3)$ Rechenoperationen. Das gleiche gilt für die Inversion einer (n,n)-Matrix. Wir wollen den Straßen-Algorithmus vorstellen, der beide Aufgaben in $\mathrm{O}(n^{\log_2 7})$, $\log_2 7 = \ell n7/\ell n2 = 2.807$, Rechenoperationen erledigt.

Für eine (n,n)-Matrix A mit geradem n schreiben wir

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$$

mit $(\frac{n}{2}, \frac{n}{2})$-Matrizen A_{ij}.

Lemma 1.2.1 *Sei $C = AB$ mit (n,n)-Matrizen A, B, C. Dann gilt*

$$\begin{array}{lclclcl} C_{11} & = & I + IV - V + VII & , & C_{12} & = & III + V \ , \\ C_{21} & = & II + IV & , & C_{22} & = & I + III - II + VI \end{array}$$

mit

$$\begin{array}{lcl} I & = & (A_{11} + A_{22})(B_{11} + B_{22}) \\ II & = & (A_{21} + A_{22})B_{11} \\ III & = & A_{11}(B_{12} - B_{22}) \\ IV & = & A_{22}(B_{21} - B_{11}) \\ V & = & (A_{11} + A_{12})B_{22} \\ VI & = & (A_{21} - A_{11})(B_{11} + B_{12}) \\ VII & = & (A_{12} - A_{22})(B_{21} + B_{22}) \end{array}$$

Beweis: Der Beweis durch einfaches Nachrechnen ist trivial.

Wer Schwierigkeiten hat, sei auf V. Straßen: Gaussian *Elimination ist not optimal*, Numer. Math. **13**, 354-356 (1969), verwiesen.

□

Satz 1.2.2 *Sei $n = 2^p$. Dann kann man zwei (n,n)-Matrizen in $O(n^{\log_2 7})$ Rechenoperationen multiplizieren.*

Beweis: Inspektion der Formel von Lemma 1.2.1 zeigt, daß man die Multiplikation zweier (n,n)-Matrizen durch 7 Multiplikationen und 18 Additionen von $(\frac{n}{2},\frac{n}{2})$-Matrizen ausführen kann. Ist also $n = m \cdot 2^p$ und M_p bzw. A_p die Anzahl der reellen Multiplikation bzw. Additionen, welche man zur Multiplikation zweier (n,n)-Matrizen benötigt, so gilt nach Lemma 1.2.1

$$\begin{aligned} M_{p+1} &\le 7M_p &, \quad M_0 \le m^3 \,, \\ A_{p+1} &\le 7A_p + 18(m \cdot 2^p)^2 &, \quad A_0 \le m^3 \,. \end{aligned}$$

Nach Lemma 1.1.1 erhält man

$$\begin{aligned} M_p &\le 7^p m^3 \\ A_p &\le 7^p m^3 + 18m^2 \sum_{j=0}^{p-1} 7^{p-1-j} 2^{2j} \\ &= 7^p m^3 + 18m^2 7^{p-1} \sum_{j=0}^{p-1} (\tfrac{4}{7})^j \\ &\le 7^p(m^3 + 6m^2) \end{aligned}$$

Für $m = 1$ folgt wegen $7^p = n^{\log_2 2}$ die Behauptung.

□

Für $n = m2^p$ lautet der Straßen-Algorithmus

fmamu (n, A, B, C)
{ if $(n \le = m)$ Schulmethode;
else
{ fmamu $(\frac{n}{2}, A_{11} + A_{22}, B_{11} + B_{22}, I)$;
⋮
fmamu $(\frac{n}{2}, A_{12} - A_{22}, B_{21} + B_{22}, VII)$;
$C_{11} = I + IV - V + VII$; $C_{12} = III + V$;
$C_{21} = II + IV$; $C_{22} = I + VI - II + VI$;
}
}

Nun zur Matrizeninversion. Anstelle von Lemma 1.2.1 haben wir jetzt

Lemma 1.2.3 *Sei A eine invertierbare (n,n)-Matrix mit geradem n, und seien die Matrizen A_{11} und $A_{21}A_{11}^{-1}A_{12} - A_{22}$ invertierbar. Dann gilt mit*

$$\begin{array}{rclcrclcrcl} I &=& A_{11}^{-1} &,& II &=& A_{21}I &,& III &=& IA_{12} \\ IV &=& A_{21}III &,& V &=& IV - A_{22} &,& VI &=& V^{-1} \end{array}$$

für $C = A_{-1}$:

$$\begin{array}{rclcrclcrcl} C_{12} &=& III\,VI &,& C_{12} &=& VI\,II &,& VII &=& III\,C_{21}\,, \\ C_{11} &=& I - VII &,& C_{22} &=& -VI &. \end{array}$$

Beweis: Durch triviales Nachrechnen.

□

Satz 1.2.4 *Sei $n = 2^p$ und A eine invertierbare (n,n)-Matrix. Unter der Voraussetzung V (siehe unten) kann A mit $O(n^{\log 7/\log 2})$ Rechenoperationen invertiert werden.*

Beweis: Durch Inspektion der Formeln von Lemma 1.2.3 sehen wir, daß eine (n,n)-Matrix durch 2 Inversionen, 6 Multiplikationen, und 2 Additionen von $(\frac{n}{2}, \frac{n}{2})$-Matrizen invertiert werden kann. Setzen wir wieder $n = m2^p$ und bezeichnen wir mit δ_p, μ_p, α_p die Anzahl der reellen Divisionen, Multiplikationen und Additionen für die Inversion einer (n,n)-Matrix, so gilt also

$$\begin{array}{lcl} \delta_{p+1} \le 2\delta_p &,& \delta_0 \le m\;, \\ \mu_{p+1} \le 2\mu_p + 6M_p &,& \mu_0 \le m^3\,, \\ \alpha_{p+1} \le 2\alpha_p + 6A_p + 2(m2^p)^2 &,& \alpha_0 \le m^3\,. \end{array}$$

Die Ungleichungen für $p = 0$ gelten, falls man für $p = 0$ das Eliminationsverfahren verwendet. Auf diese Rekursionen wenden wir wieder Lemma 1.1.1 an und erhalten

$$\begin{array}{rcl}
\delta_p & \leq & m^3 \, , \\
\mu_p & \leq & 2^p m^3 + 6 \sum_{j=0}^{p-1} M_j 2^{p-j-1} \\
 & \leq & 2^p m^3 + 6m^3 \sum_{j=0}^{p-1} 7^j 2^{p-j-1} \\
 & = & 2^p m^3 \left(1 + 3 \sum_{j=0}^{p-1} (\frac{7}{2})^j \right) \\
 & = & 2^p m^3 \left(1 + 3 \frac{(7/2)^p - 1}{\frac{7}{2}} \right) \\
 & \leq & 7^p m^3 \cdot \frac{6}{5} \, , \\
\alpha_p & \leq & \left(\frac{6}{5} m^3 + 5m^2 \right) 7^p \, .
\end{array}$$

Für $m = 1$ erhält man die Behauptung.

Natürlich können nur solche Matrizen auf diese Weise invertiert werden, für die bei allen Unterteilungen $n \to \frac{n}{2} \to \frac{n}{4} \ldots \to m$ die Voraussetzungen von Lemma 1.2.3 erfüllt sind. Dies ist Inhalt der Voraussetzung V.

$\square$