max planck institut
informatik

Multiplikation großer Zahlen Schneller als in der Schule

Vorlesung basiert auf Beitrag von Eigenwillig/Mehlhorn im Taschenbuch der Algorithmen

Kurt Mehlhorn and Kosta Panagiotou

Max-Planck-Institut für Informatik und Universität des Saarlandes

21. Oktober 2011

Lernziele

- die vertraute Lösung ist nicht immer die beste; man kann schneller multiplizieren als das die Menschheit für 2000 Jahre gemacht hat.
- Die algorithmische Technik Teile und Beherrschen.
- Die Programmiertechnik Rekursion.
- Vertiefung von Schritte zählen.

Multiplizieren

Um zwei ganze Zahlen a und b miteinander zu multiplizieren, multipliziert man a mit jeder Ziffer von b und arrangiert diese Teilprodukte in einem Stufenschema. Dann addiert man die Teilprodukte spaltenweise.

$$
\begin{array}{r}
5678 \cdot 4321 \\
\hline
22712 \\
17034 \\
11356 \\
5678 \\
\hline
24534638
\end{array}
$$

Wir nennen diese Methode die *Schulmethode der Multiplikation*.

Fragen

Wie aufwendig ist die Schulmethode zur Multipliation?
Können wir mit weniger Aufwand multiplizieren?

Warum?

Praxis: Schnelles Rechnen mit langen Zahlen braucht man in vielen Anwendungsgebieten der Informatik, zum Beispiel beim Verschlüsseln von Nachrichten und bei der zuverlässigen Lösung geometrischer Probleme.
Theorie: Die Schulmethode der Multiplikation erscheint uns so vertraut und natürlich, dass jede wesentliche Verbesserung – und wir werden eine solche kennen lernen – eine bemerkenswerte Überraschung ist.
Ist Multiplizieren schwerer als Addieren?

Grundoperationen

Wir messen Aufwand in Grundoperationen (kleines EinmalEins)

Multiplikation von zwei Ziffern:

gegeben Ziffern x und y, berechne die zwei Ziffern u und v ihres Produkts: $x \cdot y = 10 \cdot u + v$.
Beispiel: Für $x = 3$ und $y = 7$ wissen wir
$x \cdot y = 3 \cdot 7 = 21 = 10 \cdot 2 + 1$, also $u = 2$ und $v = 1$.

Addition von drei Ziffern:

gegeben drei Ziffern, berechne die zwei Ziffern ihrer Summe:
$x + y + z = 10 \cdot u + v$.
Beispiel: Für $x = 3$, $y = 5$ und $z = 4$ haben wir $u = 1$ und $v = 2$, weil $3 + 5 + 4 = 12 = 10 \cdot 1 + 2$.

Wieviele Grundoperationen braucht die Multiplikation?

Addition zweier Zahlen a und b aus je n Ziffern

Wir schreiben sie untereinander (wenn eine kürzer ist, füge vorne Nullen an) und addieren von rechts nach links die Ziffern in jeder Spalte mit der oben eingeführten Ziffern-Addition. Vom Ergebnis $10 \cdot u + v$ schreiben wir die Ziffer v als Ergebnisziffer hin; die Ziffer u schreiben wir als dritte Ziffer (Übertrag) bei der nächsten Spalte dazu.

$$\begin{array}{r} 6917 \\ 4269 \\ \hline 1101 \\ \hline 11186 \end{array}$$

Insgesamt haben wir dann n Grundoperationen durchgeführt, nämlich eine Ziffern-Addition für jede Spalte.

Multiplikation einer Zahl a mit einer Ziffer y

Wir gehen von rechts nach links die Ziffern von a durch. Jede Ziffer x von a multiplizieren wir mit y. Das Ergebnis $10 \cdot u + v$ schreiben wir in eine neue Zeile, und zwar so, dass v in derselben Spalte wie x steht und u links daneben. Anschließend addieren wir alle diese zweistelligen Zwischenergebnisse.

$$
\begin{array}{r}
5\,6\,7\,8 \cdot 4 \\
\hline
\quad 3\,2 \\
\quad 2\,8 \\
\quad 2\,4 \\
2\,0 \\
0\,0\,1\,0 \\
\hline
2\,2\,7\,1\,2
\end{array}
$$

Aufwand für Multiplikation “Zahl mal Ziffer”

$$
\begin{array}{r}
5\,6\,7\,8 \cdot 4 \\
\hline
\quad 3\,2 \\
\quad 2\,8 \\
\quad 2\,4 \\
2\,0 \\
0\,0\,1\,0 \\
\hline
2\,2\,7\,1\,2
\end{array}
$$

Für jede der n Ziffern von a, eine Ziffern-Multiplikation.

dann $n + 1$ Spalten von Zwischenergebnisse addieren.
rechteste Spalte: keine Arbeit.
In den anderen n Spalten eine Ziffern-Addition.

Gesamtaufwand $2 \cdot n$

Schulmultiplikation von zwei Zahlen a und b mit je n Ziffern

Für jede Ziffer y von b berechne Teilprodukt $a \cdot y$: $2 \cdot n$ GOPs.

$$
\begin{array}{r}
5\,6\,7\,8 \cdot 4\,3\,2\,1 \\
\hline
2\,2\,7\,1\,2\,0\,0\,0 \\
0\,1\,7\,0\,3\,4\,0\,0 \\
0\,0\,1\,1\,3\,5\,6\,0 \\
0\,0\,0\,0\,5\,6\,7\,8 \\
\hline
2\,4\,5\,3\,4\,6\,3\,8
\end{array}
$$

Aufwand für alle Teilprodukte: $2 \cdot n^2$ GOPs, da b n Ziffern hat.

Aufsummieren der Teilprodukte

$$
\begin{array}{r}
5\,6\,7\,8 \cdot 4\,3\,2\,1 \\
\hline
2\,2\,7\,1\,2\,0\,0\,0 \\
0\,1\,7\,0\,3\,4\,0\,0 \\
0\,0\,1\,1\,3\,5\,6\,0 \\
0\,0\,0\,0\,5\,6\,7\,8 \\
\hline
2\,4\,5\,3\,4\,6\,3\,8
\end{array}
$$

Addition der Teilprodukte: Erst addieren wir die erste Zeile zur zweiten Zeile, zu dieser Zwischensumme addieren wir die dritte Zeile, und so weiter, bis wir schließlich alle n Teilprodukte (Zeilen) addiert haben, also $n-1$ Additionen langer Zahlen:

Im Beispiel ist $n = 4$:

$$
\begin{aligned}
22712000 + 1703400 &= 24415400, \\
24415400 + 113560 &= 24528960 \\
24528960 + 5678 &= 24534638.
\end{aligned}
$$

Aufwand der Summierphase und Gesamtaufwand

$$
\begin{array}{r}
5\,6\,7\,8 \cdot 4\,3\,2\,1 \\
\hline
2\,2\,7\,1\,2\,0\,0\,0 \\
0\,1\,7\,0\,3\,4\,0\,0 \\
0\,0\,1\,1\,3\,5\,6\,0 \\
0\,0\,0\,0\,5\,6\,7\,8 \\
\hline
2\,4\,5\,3\,4\,6\,3\,8
\end{array}
$$

Das Endergebnis $a \cdot b$ hat höchstens $2 \cdot n$ Ziffern.
Zwischenergebnisse sind auch nicht länger.

Jede Addition braucht höchstens $2 \cdot n$ GOPs.

$n - 1$ Additionen: $(n-1) \cdot (2 \cdot n) = 2 \cdot n^2 - 2 \cdot n$ GOPs.

Gesamtaufwand: $4 \cdot n^2 - 2 \cdot n$ GOPs.

Was bedeutet das konkret?

Gesamtaufwand: $4 \cdot n^2 - 2 \cdot n$ GOPs

$n = 100.000$ Ziffern: fast 40 Milliarden GOPs,
1 Million Ziffern: fast 4 Billionen GOPs.

n	Schule	Karatsuba4	Karatsuba32
100	0.000216638	0.000573723	0.000145455
1600	0.0542105	0.0459091	0.0126582
3200	0.218	0.13875	0.0384615
51200	55.71	11.11	3.11
102400	223.33	33.36	9.29
204800	900.98	100.72	27.91

Laufzeiten in Sekunden auf KMs Notebook in 2007.

Methode von Karatsuba (1962): Multiplikation von Zahlen der Länge zwei

$$a = a_1 \cdot 10 + a_0 \quad \text{und} \quad b = b_1 \cdot 10 + b_0.$$

Dann

$$\begin{aligned} a \cdot b &= (a_1 \cdot 10 + a_0) \cdot (b_1 \cdot 10 + b_0) \\ &= (a_1 \cdot b_1) \cdot 100 + (a_1 \cdot b_0 + a_0 \cdot b_1) \cdot 10 + a_0 \cdot b_0. \end{aligned}$$

Beispiel ($a = 78$ und $b = 21$):

$$78 \cdot 21 = (7 \cdot 2) \cdot 100 + (7 \cdot 1 + 8 \cdot 2) \cdot 10 + 8 \cdot 1 = 1638.$$

Produkt der zweistelligen Zahlen a und b = **vier** Multiplikationen einstelliger Zahlen und Addition der Ergebnisse.

Karazuba: es geht auch mit **drei** Multiplikationen

Karazuba: es geht auch mit drei Multiplikationen

$$\begin{array}{lrcl} \text{berechne} & u & = & a_1 \cdot b_1, \\ & v & = & (a_0 - a_1) \cdot (b_0 - b_1), \\ & w & = & a_0 \cdot b_0. \end{array}$$

Aber warum hilft das? Weil folgende Gleichung gilt:

$$u + w - v = a_1 \cdot b_1 + a_0 \cdot b_0 - (a_0 - a_1) \cdot (b_0 - b_1) = a_1 \cdot b_0 + a_0 \cdot b_1.$$

Und daher:

$$a \cdot b = u \cdot 10^2 + (u + w - v) \cdot 10 + w.$$

Beispiel $a = 78$ und $b = 21$: Es ist

$$u = 7 \cdot 2 = 14, \quad v = (8 - 7) \cdot (1 - 2) = -1, \quad w = 8 \cdot 1 = 8.$$

Damit finden wir

$$78 \cdot 21 = 14 \cdot 100 + (14 + 8 - (-1)) \cdot 10 + 8 = 1400 + 230 + 8 = 1638.$$

Die Methode von Karazuba für beliebig lange Zahlen

Zwei Zahlen a und b der Länge $n = 2 \cdot 2 \cdot 2 \cdots 2 = 2^k$:

$$a = a_1 \cdot 10^{n/2} + a_0 \quad \text{und} \quad b = b_1 \cdot 10^{n/2} + b_0$$

Berechne Produkt mit drei Multiplikationen von Zahlen der Länge $\frac{n}{2} = 2^{k-1}$ in der Art

$$a \cdot b = a_1 \cdot b_1 \cdot 10^n + (a_1 \cdot b_1 + a_0 \cdot b_0 - (a_0 - a_1) \cdot (b_0 - b_1)) \cdot 10^{n/2} + a_0 \cdot b_0$$

Anzahl der Ziffer-Multiplikationen zur Multiplikation von Zahlen der Länge 2^k =
dreimal (statt viermal) Anzahl für Zahlen der Länge 2^{k-1}.

Anzahl der Ziffer-Multiplikationen zur Multiplikation von Zahlen der Länge 2^k =
dreimal (statt viermal) Anzahl für Zahlen der Länge 2^{k-1}.

Länge	Karazuba	Schulmethode
$1 = 2^0$	1	1
$2 = 2^1$	3	4
$4 = 2^2$	9	16
$512 = 2^9$	19.638	262.144
$1.024 = 2^{10}$	59.049	1.048.576
$1.048.576 = 2^{20}$	3.486.784.401	1.099.511.627.776
n	$n^{\log 3} = n^{1,58\ldots}$	n^2

vorletzte Zeile: Karazuba = Schulmethode/287
Vergleich: 1 Sekunde = 5 Minuten/300

Das Prinzip Teile und Beherrsche

Die Aufgabe "multipliziere zwei Zahlen der Länge n" wird zurückgeführt auf mehrere Aufgaben von der gleichen Art, aber von kleinerer Größe, nämlich: „multipliziere zwei Zahlen der Länge $\frac{n}{2}$“.

Damit verkleinern wir das Problem so lange, bis es ganz einfach geworden ist („multipliziere zwei Ziffern“).

Programmiertechnik: Rekursion

```
integer Karatsuba(integer a, integer b)
{ int n = a.size(); int m = b.size(); assert(n == m);
integer p(2*n);
if (n < 4) return mult(a,b);
int k = n/2; integer a0(k), a1(n - k), b0(k), b1(n - k);
split(a,a1,a0); split(b,b1,b0);
integer p2 = Karatsuba(a1,b1),
p1 = Karatsuba(add(a1,a0),add(b1,b0)),
p0 = Karatsuba(a0,b0);
for (int i = 0; i < 2*k; i++) p[i] = p0[i];
for (int i = 2*k; i < n+m; i++) p[i] = p2[i - 2*k];
sub(p1,p0); sub(p1,p2); add_at(p,p1,k);
return p;
}
```

Aktuelle Forschung

- es wurden seither noch wesentlich schnellere Verfahren gefunden
  - Schönhage und Strassen (71): $n \cdot \log n \cdot \log(\log n)$
  - Führer (2007): $n \cdot \log n \cdot 2^{O(\log^* n)}$.
- in eingeschränktem Modell: $n \log n$ untere Schranke
- Offenes Problem: Ist Multiplizieren beweisbar schwerer als Addieren?

Geometrisches Rechnen

Schnitt Ellipse $(x - \sqrt{2})^2 + 2\,(y - \sqrt{3})^2 = 5$
und Gerade $y = d - 2x$.

Wird die Ellipse von der Geraden geschnitten?
Wenn ja, in zwei Punkten oder tangential?

Schnitt Ellipse $(x - \sqrt{2})^2 + 2\,(y - \sqrt{3})^2 = 5$

und Gerade $y = d - 2x$. Einsetzen von $y =$ … in Ellipsengleichung gibt qudratische Gleichung für x.

$a\,x^2 + \mathrm{b}\,\mathrm{x} + \mathrm{c} = 0$ hat zwei, eine, keine Lösung, wenn

$$D = b^2 - 4\mathrm{ac} >= < 0$$

Hier $D = -2d^2 + (68\sqrt{3} + 8\sqrt{2})\mathrm{d} + 23 + 8\sqrt{6}$

d = 0, d = 1000

Hier $D = -2d^2 + (68\sqrt{3} + 8\sqrt{2})\mathrm{d} + 23 + 8\sqrt{6}$

Aber was ist für $d = 17\sqrt{3} + 2\sqrt{2} + \sqrt{(1783 + 144\sqrt{6})/6}$

Methode 1: einsetzen und vereinfachen

Methode 2: durch numerisches Rechnen

Hier $D = -2d^2 + (68\sqrt{3} + 8\sqrt{2})\mathrm{d} + 23 + 8\sqrt{6}$

Aber was ist für $d = 17\sqrt{3} + 2\sqrt{2} + \sqrt{(1783 + 144\sqrt{6})/6}$

Satz (FMSS): Sei D ein Ausdruck mit ganzzahligen Operanden und Operatoren +, -, *, und Wurzel.

Dann D = 0 oder $|D| \geq \frac{1}{u^{2^k}}$

K = Anzahl der (verschiedenen) Wurzeln in E

u ≥ Wert von E nach Ersetzen von – durch +

Hier $D = -2d^2 + (68\sqrt{3} + 8\sqrt{2})\mathrm{d} + 23 + 8\sqrt{6}$

Aber was ist für $d = 17\sqrt{3} + 2\sqrt{2} + \sqrt{(1783 + 144\sqrt{6})/6}$

Dann D = 0 oder $|D| \geq \frac{1}{u^{2^k}}$

K = Anzahl der (verschiedenen) Wurzeln in E hier k =

u ≥ Wert von E nach Ersetzen von – durch +

d ≤ 34 + 4 + Wurzel aus (1783 + 432)/2 ≤ 80

D ≤ 2* 6400 + (140 + 16)*80 + 47 ≤ 30000 = u

Also D = 0 oder $|D| \geq 1/(30000^8) \geq 1/(10^{40})$

Hier $D = -2d^2 + (68\sqrt{3} + 8\sqrt{2})\mathrm{d} + 23 + 8\sqrt{6}$

Aber was ist für $d = 17\sqrt{3} + 2\sqrt{2} + \sqrt{(1783 + 144\sqrt{6})/6}$

Also D = 0 oder |D| ≥ $1/(30000^8) \geq 1/(10^{40})$.

Berechne D mit 40 + Stellen nach dem Komma.

Wurzel aus a durch Newtoniteration

$$x_0 = a \quad x_{i+1} = (x_i + \frac{a}{x_i})/2$$

Wurzel aus a durch Newtoniteration

$$x_0 = a \quad x_{i+1} = (x_i + \frac{a}{x_i})/2$$