

# Diskrete Strukturen und Logik

WiSe 2007/08 in Trier

Henning Fernau

Universität Trier

fernau@uni-trier.de

**Was wir alles können**

Rückblick, Einblick, Ausblick, . . .

**Rechnerarithmetik:** *Gleitkommafilter* nach Fortune / v.Wyk

**Problem:** Wie kann man Punktkoordinaten für geometrische Aufgaben sinnvoll im Rechner speichern, um insbesondere **verlässlich** feststellen zu können, auf welcher Seite einer Geraden ein Punkt liegt? Dies genau entscheiden zu können ist **wichtig** für die Korrektheit vieler geometrischer Algorithmen (Sweep Line).

Eingebaute `double`-Arithmetik liefert schnelle, aber manchmal **falsche** Lösung.

**Mögliche Lösung:** Stelle Punkte als Paare **rationaler Zahlen** dar, und zwar mit beliebiger Genauigkeit.

**Schwierigkeit** (gegenüber der in den Prozessoren eingebauten `double`-Arithmetik): Rechnen wird seeeehr langsam

## Darstellung von 64-Bit-Gleitkommazahlen (double nach IEEE Standard)

$$x = \pm M \cdot 2^e.$$

$\pm$ : Vorzeichenbit

M: 53 Bit Mantisse

e: 11 Bit Exponent

$\tilde{a}$ : Gleitkommadarstellung von  $a \in \mathbb{R}$

**Beispiel:**  $a = 0, \boxed{1011001 \dots 1} \times \dots \cdot 2^e$

$\rightsquigarrow \tilde{a} = 0, \boxed{1011001} \cdot 2^e$ , falls  $x = 0$

$\rightsquigarrow \tilde{a} = 0, \boxed{1011010} \cdot 2^e$ , falls  $x = 1$  (Runden)

Wieso reichen 64 Bit ?!

## Gleitkommafilter Grundgedanke

Benutze eingebaute schnelle Gleitkommaarithmetik, solange die dadurch gemachten Fehler für die Entscheidungen des Algorithmus nicht beeinflussen.

Sollte die Genauigkeit von `double` für Entscheidungen ungenügend sein, so muss man auf exakte (langsame) Zahldarstellungen ausweichen.

Das tritt hoffentlich nur selten auf.

Für Zahlen (Ausdrücke), die *nur unterwegs* als Zwischenergebnisse von Rechnungen auftreten, haben wir also zwei Darstellungen:  $E$  und  $\tilde{E}$ .

Hoffentlich müssen wir aber  $E$  nicht wirklich ausrechnen.

## Genauigkeitsabschätzungen

Für *richtige* Zahlen gilt:  $|a - \tilde{a}| \leq \frac{1}{2} \cdot 2^{-53} \cdot 2^e$ .

Hierbei ist  $\epsilon = 2^{-53}$  die *Maschinengenauigkeit*,

$i(a) = \frac{1}{2}$  der *Rundungsfehler* und  $m(a) = 2^e$  der *Zahlbereich*.

Für Ausdruck E soll allgemein gelten:

(1)  $|E| \leq m(E)$ ,  $|\tilde{E}| \leq m(E)$ ;  $m(E)$  ist Zweierpotenz.

(2)  $|E - \tilde{E}| \leq i(E)\epsilon m(E)$ . *Fehlerabschätzung*

## **Fehlerabschätzungen**, strukturell induktiv

(über den rekursiven Aufbau arithmetischer Ausdrücke)

**Satz:** (a) Für  $E = E_1 \pm E_2$  gilt:

$$\begin{aligned}m(E) &= 2 \cdot \max(m(E_1), m(E_2)) \\i(E) &= 1 + \frac{i(E_1) + i(E_2)}{2}\end{aligned}$$

(b) Für  $E = E_1 \cdot E_2$  gilt:

$$\begin{aligned}m(E) &= m(E_1)m(E_2) \\i(E) &= 1 + i(E_1) + i(E_2)\end{aligned}$$

**Vorteil:** Berechnung der Fehlerabschätzung parallel zur eigentlichen `double`-Arithmetik ist schnell.

## Fehlerabschätzungen, strukturell induktiv

Der IEEE-Standard legt (*axiomatisch*) u.a. folgende zwei Eigenschaften der Gleitkomma-Addition  $\oplus$  fest:

$$\tilde{a} \oplus \tilde{b} = (1 + \varepsilon)(a + b) \text{ mit } |\varepsilon| \leq \epsilon.$$

$\oplus$  ist *monoton*

Beweis: Wir zeigen leglich (a) durch strukturelle Induktion. Als Induktionsanker haben wir uns die Aussage bereits für einzelne Zahlen  $E = a$  überlegt.

Wir nehmen daher an, dass die Behauptung für  $E_1$  und  $E_2$  gilt.

Betrachte

$$\begin{aligned} |\tilde{E}| &= |\tilde{E}_1 \oplus \tilde{E}_2| \\ &\leq m(E_1) \oplus m(E_2) \\ &\leq \max(m(E_1), m(E_2)) \oplus \max(m(E_1), m(E_2)) \\ &= 2 \cdot \max(m(E_1), m(E_2)) \end{aligned}$$

Die erste Ungleichung gilt nach Induktionsannahme, die zweite wegen der Monotonie von  $\oplus$  und die dritte wiederum nach Induktionsannahme, da  $m(E_i)$  Zweierpotenzen sind.



Da mit  $m(E_i)$  auch  $2 \cdot \max(m(E_1), m(E_2))$  Zweierpotenzen sind, gilt die Behauptung über  $m(E) = 2 \cdot \max(m(E_1), m(E_2))$ .

Für die Fehlerabschätzung rechne:

$$\begin{aligned}
 |\tilde{E} - E| &= |\tilde{E}_1 \oplus \tilde{E}_2 - E| \\
 &= |(1 + \varepsilon)(\tilde{E}_1 + \tilde{E}_2) - E| \\
 &= |(E_1 + (\tilde{E}_1 - E_1)) + (E_2 + (\tilde{E}_2 - E_2)) - E + \varepsilon(\tilde{E}_1 + \tilde{E}_2)| \\
 &\leq |\tilde{E}_1 - E_1| + |\tilde{E}_2 - E_2| + \varepsilon(|\tilde{E}_1| + |\tilde{E}_2|) \\
 &\leq i(E_1)\varepsilon m(E_1) + i(E_2)\varepsilon m(E_2) + \varepsilon(m(E_1) + m(E_2)) \\
 &\leq (i(E_1) + i(E_2))\varepsilon \max(m(E_1), m(E_2)) + 2 \cdot \max(m(E_1), m(E_2))\varepsilon \\
 &= i(E)\varepsilon m(E)
 \end{aligned}$$

Welche Eigenschaften wurden bei dieser Abschätzung verwendet ?

**Noch ein geometrisches Problem**, das für die Laufzeitabschätzung gewisser geometrischer Algorithmen wichtig ist: *Anzahl Schnittpunkte k-ter Ordnung*.

Betrachte Menge  $L$  mit  $n$  Geraden in der Ebene, von denen keine zwei parallel sind und von denen keine drei sich in einem gemeinsamen Punkt schneiden.

Es sei  $o$  ein Punkt, der auf keiner der Geraden aus  $L$  liegt.

Wir diskutieren die Schnittpunkte aller Geraden aus  $L$ .

Nach Voraussetzung gibt es insgesamt  $\binom{n}{2}$  Schnittpunkte.

Die *Ordnung* eines Schnittpunkts  $v$  sei  $k$ , wenn die Strecke  $ov$  zusätzlich zu den zwei Geraden, die sich in  $v$  schneiden, genau  $k$  weitere Geraden aus  $L$  schneidet.

**Frage:** Was ist bei gegebenen  $n, k$  die größtmögliche Anzahl Schnittpunkte der Ordnung **höchstens  $k$**  ?

## Der Fall $k = 0$ :

Die Geraden aus  $L$  teilen die Ebene in Zellen ein.

Die Schnittpunkte nullter Ordnung sind gerade die Eckpunkte derjenigen Zelle, die  $o$  enthält.

Jede Gerade kann diese Zelle nur höchstens einmal beranden

$\rightsquigarrow$  Es gibt  $\leq n$  Schnittpunkte nullter Ordnung.

Wir werden durch ein Wahrscheinlichkeitsargument den allgemeinen Fall auf diesen Spezialfall zurückführen (nicht durch Induktion).

Dies ist ein weiteres Beispiel für ein *probabilistisches Argument*.

## Ein Wahrscheinlichkeitsmodell für den allgemeinen Fall

Sei  $p \in (0, 1)$ ; die genaue Festlegung erfolgt später.

Wir wählen eine Teilmenge  $R \subseteq L$  von Gerade wie folgt: Gerade  $\ell \in L$  wird mit Wahrscheinlichkeit  $p$  ausgewählt, mit Wahrscheinlichkeit  $(1 - p)$  nicht.

Formal besteht der Wahrscheinlichkeitsraum also aus allen Teilmengen  $R \in 2^L$ , und  $R$  wird mit Wahrscheinlichkeit  $p^{|R|}(1 - p)^{n-|R|}$  gezogen, mit  $n = |L|$ .

Annahme: nur die Geraden aus  $R$  sind in der Ebene gezeichnet.

Betrachte Zufallsvariable  $f(R)$ , die die Anzahl der Geraden angibt, die bezüglich  $R$  nullte Ordnung haben.

M.a.W.:  $f(R)$  zählt die Schnittpunkte von Geraden aus  $R$ , deren Sicht von  $o$  aus von keiner Geraden aus  $R$  verstellt wird.

Wir schätzen den Erwartungswert  $E[f]$  auf zweierlei Arten ab.

## Erste Abschätzung von $E[f]$ :

Da wir nur Geraden aus  $R$  zählen, gilt  $f(R) \leq |R|$ .

Da der Erwartungswert monoton ist und da  $g(R) = |R|$  ebenfalls als Zufallsvariable aufgefasst werden kann, gilt:

$$E[f] \leq E[g].$$

Im Rahmen der Diskussion der geometrischen Verteilung haben wir  $E[g]$  bereits einmal berechnet.

Daher wissen wir:  $E[g] = pn$ .

$$\leadsto \boxed{E[f] \leq pn}.$$

## Zweite Abschätzung von $E[f]$ :

Für jeden Schnittpunkt  $v$  definiere Ereignis  $A_{\mathcal{R}}(v)$ , das genau dann eintritt, wenn  $v$  bezüglich der Geraden aus  $\mathcal{R}$  einer der Schnittpunkte nullter Ordnung ist.

Also tritt  $A_{\mathcal{R}}(v)$  genau dann ein, wenn  $v$  zu  $f(\mathcal{R})$  Eins beiträgt.

M.a.W.:  $f(\mathcal{R}) = |A_{\mathcal{R}}|$ .

$A_{\mathcal{R}}(v)$  tritt genau dann ein, wenn die folgenden zwei Bedingungen erfüllt sind:

1. Die beiden Geraden, deren Schnittpunkt  $v$  ist, liegen in  $\mathcal{R}$ .
2. Keine der Geraden, die die Strecke  $ov$  in einem inneren Punkt schneiden, liegt in  $\mathcal{R}$ .

$\leadsto P(A_{\mathcal{R}}(v)) = p^2(1 - p)^{\ell(v)}$ , wobei  $\ell(v)$  die Ordnung des Schnittpunktes  $v$  bezeichnet.

## Analyse

$M$ : Menge aller Schnittpunkte von Geraden aus  $L$ :

$M_k \subseteq M$ : Menge aller Schnittpunkte höchstens  $k$ -ter Ordnung

$$\begin{aligned} E[f] &= E\left[\bigcup_{v \in M} [v \in A_r]\right] = \sum_{v \in M} E[v \in A_r] = \sum_{v \in M} P(A_r(v)) \geq \sum_{v \in M_k} P(A_r(v)) \\ &= \sum_{v \in M_k} p^2(1-p)^{\ell(v)} \geq \sum_{v \in M_k} p^2(1-p)^k = |M_k|p^2(1-p)^k \end{aligned}$$

Beide Abschätzungen zusammen liefern:

$$\boxed{np \geq E[f] \geq |M_k|p^2(1-p)^k.} \quad \text{Daraus folgt:}$$

$$|M_k| \leq \frac{n}{p(1-p)^k}$$

Wir haben noch einen **Freiheitsgrad**: die geschickte Wahl von  $p$ .

Mit  $p = \frac{1}{k+1}$  und etwas Analysiskenntnissen folgt:

$$\left(1 - \frac{1}{k+1}\right)^k \geq \frac{1}{e} > \frac{1}{3},$$

woraus sofort die Behauptung folgt:

$$|M_k| \leq \frac{n}{\frac{1}{k+1} \left(1 - \frac{1}{k+1}\right)^k} \leq 3(k+1)n.$$



## **Warnung** vor mathematischen Manierismen nach Hans Freudenthal:

Eine *Sitzung* ist ein Elftupel  $(S, T, v, s, U, V, g, i, j, W, k)$ , bestehend aus:  
einer beschränkten Teilmenge  $S$  des Euklidischen Raumes, genannt *Sitzungsraum*,  
einer endlichen Menge  $T$  der Teilnehmer,  
zwei ausgezeichneten Elementen  $v, s \in T$  mit  $v \neq s$ , *Vorsitzender* bzw. *Schriftführer* geheißen,  
einer endlichen Menge  $U$  so genannter *Stühle*,  
einer endlichen Menge  $V$  so genannter *Tassen*,  
einem Objekt  $g$ , genannt *Glocke*,  
einer Bijektion  $i : T \rightarrow U$ ,  
einer Injektion  $j : T \rightarrow V$ ,  
einer geordneten Menge  $W$  von *Wortbeiträgen* und  
einer Abbildung  $k : W \rightarrow T$  mit der Eigenschaft, dass  $v \in k(W)$  gilt.  
Ist  $k$  gar eine Surjektion, so sagt man auch: jeder hat *das Wort erhalten*.

## Nochmal Algebra

Unsere algebraischen Kenntnisse helfen uns auch gut zu einem Grundverständnis des (für viele) auf dieser Vorlesung aufbauenden Vorlesung *Automaten und Formale Sprachen* (AFS).

Dort geht es zunächst um sogenannte reguläre Sprachen.

Was dies ist, können wir rasch erklären:

Ein *Alphabet*  $\Sigma$  ist eine endliche, nicht-leere Menge von *Zeichen*.

Ein *Wort* ist ein Element von  $\Sigma^*$ , dem von  $\Sigma$  frei erzeugten Monoid.

Die Monoidoperation  $\cdot$  heißt hierbei zumeist *Konkatenation*.

Das neutrale Element heißt das *leere Wort* und wird mit  $\lambda$  oder  $\epsilon$  notiert.

Eine *Sprache* ist eine Menge von Wörtern, also eine Menge  $L \subseteq \Sigma^*$ .

$L$  heißt *regulär*, gdw. es ein endliches Monoid  $(M, \circ, 1)$  gibt, eine endliche Menge  $F \subseteq M$  und einen Monoidmorphismus  $\phi : \Sigma^* \rightarrow M$ , so dass  $w \in L \iff \phi(w) \in F$ .

Also...

Bis zum nächsten Semester !

Viel Erfolg bei der Klausur !