Diskrete Strukturen II

„Wahrscheinlichkeit und Statistik"

Vorlesung:

Montag 10:15 - 11:45, Raum MI 00.02.001

Dienstag 10:15 - 11:00, Raum MI 00.02.001

Zentralübung:

Freitag 13:15 - 14:45, MI 00.02.001

Übungsleiter: Martin Marciniszyn und
Alexander Offtermatt-Souza

email: ds2lea@in.tum.de

Literatur: T. Schickinger, A. Steger:
Diskrete Strukturen - Band 2,
Springer Verlag 2002

Weitere Informationen:

`http://www14.in.tum.de/lehre/2003SS/ds/`

Prof. Dr. Angelika Steger

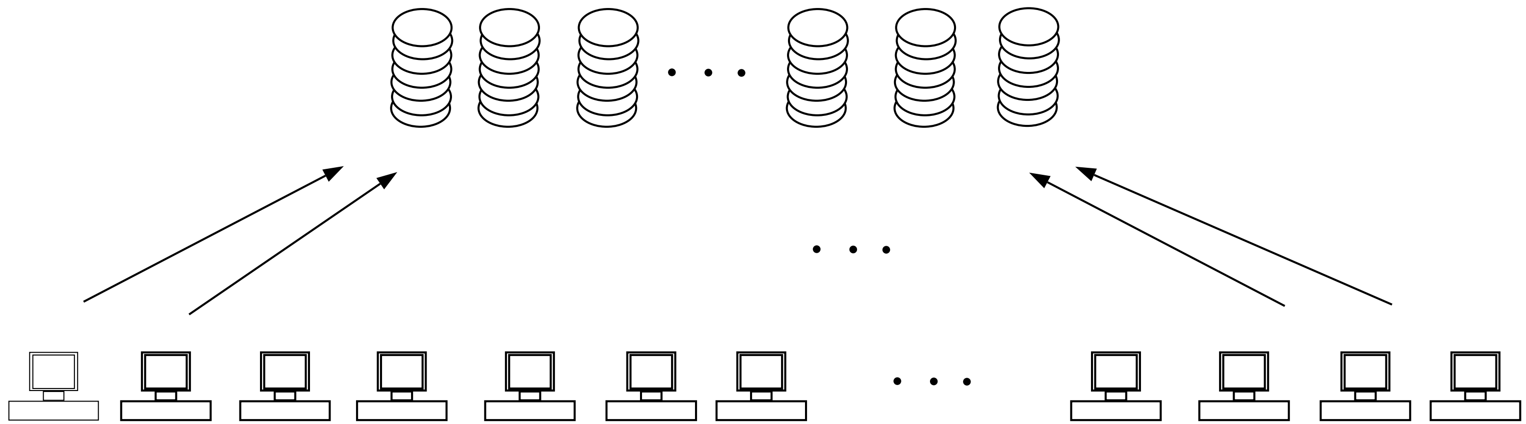
email: steger@in.tum.de

Zimmer: MI 03.09.044

Sprechstunde: Di 13-14 und nach Vereinbarung (email)

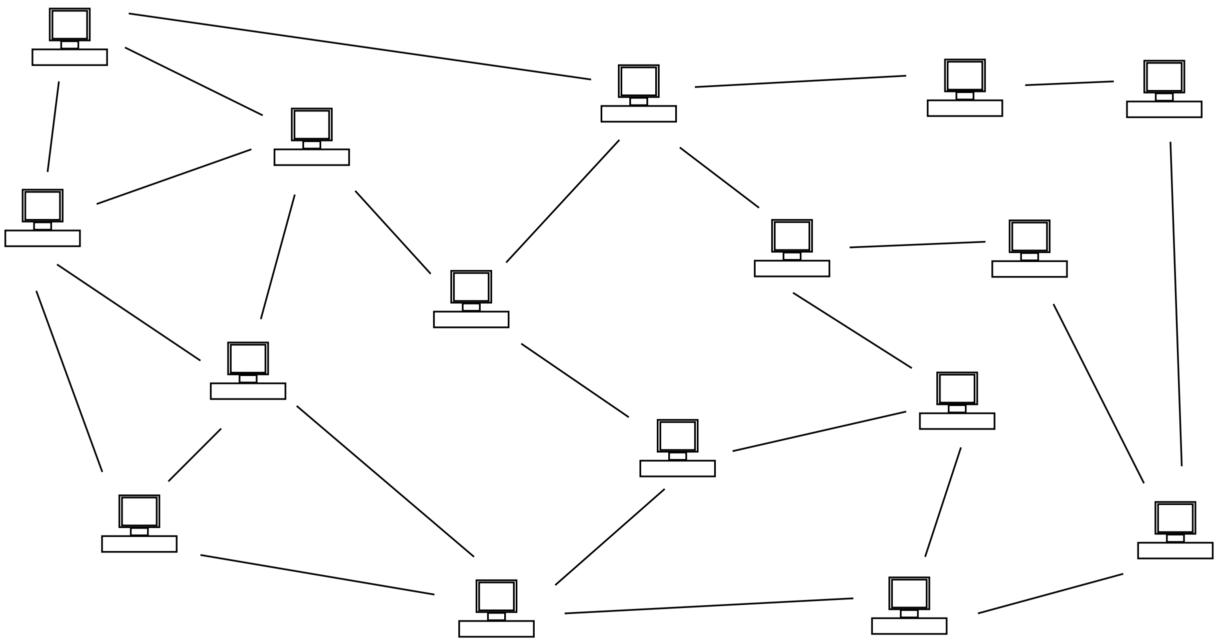
Fallbeispiel 1: Zuordnung von Datenbankanfragen

Szenario:



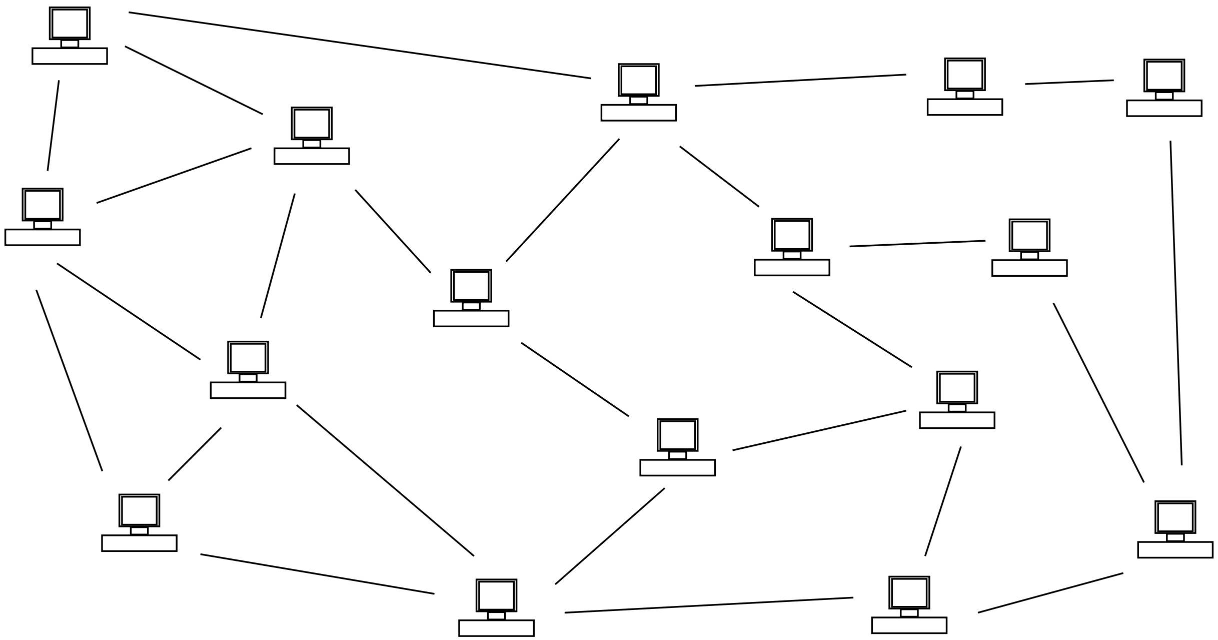
Aufgabe: Entwerfe ein möglichst einfaches Verfahren, das jede Anfrage genau einem Server zuordnet — und zwar so, daß alle Server möglichst gleich viel Arbeit erhalten.

Fallbeispiel 2: Verteilung von Information in (großen) Netzwerken



Aufgabe: Entwerfe ein möglichst einfaches Verfahren (das lokal in jedem Prozessor läuft) mit dem Informationen möglichst schnell allen Prozessoren des Netzwerkes bekannt gemacht werden können.

Fallbeispiel 3: Sicherheit in (großen) Netzwerken

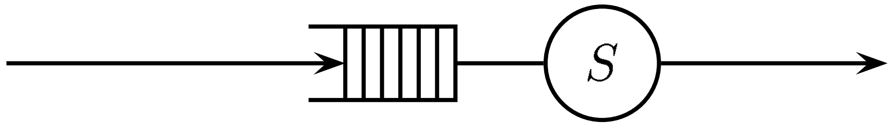


Annahme: Verbindungen zwischen zwei Rechnern brechen mit einer gewissen Wahrscheilichkeit zusammen.

Frage: Mit welcher Wahrscheilichkeit besteht dennoch immer zumindest eine Verbindung zwischen je zwei Rechnern?

Fallbeispiel 4: Warteschlagen

Szenario:



Annahme: Jobs kommen mit einer gewissen Verteilung an;
Ausführungszeit ist ebenfalls zufällig verteilt;

Fragen: Was ist die (durchschnittliche) Wartezeit in der Queue?
Wie sollten Jobs abgearbeitet werden?
(„first come first serve“ oder „round robin“ oder ...)

Fallbeispiel 5: Kryptographie

Ziel: Verschlüsseln (oder auch Authentisieren) von Information.

Näheres in der Vorlesung:

$\longrightarrow$Kryptographie

oder z.B. auch unter

http://www.rsa.com

Verschlüsselungsverfahren RSA:

Wähle zwei (etwa 768 stellige) Primzahlen p, q;

......

Frage: Wie macht man das ???

$\longrightarrow$ Durchprobieren aller möglichen Teiler ...
Dauer: etwa 10^{41} Jahre

$\longrightarrow$ Verwende ein probabilistisches Verfahren ...
Dauer: ein paar Sekunden

Definition (Diskreter Wahrscheinlichkeitsraum)

Ein *diskreter Wahrscheinlichkeitsraum* ist bestimmt durch eine *Ergebnismenge* $\Omega = \{\omega_1, \omega_2, \ldots\}$ von *Elementarereignissen*. Jedem Elementarereignis ω_i ist eine *(Elementar-)Wahrscheinlichkeit* $\Pr[\omega_i]$ zugeordnet, wobei wir fordern, dass $0 \leq \Pr[\omega_i] \leq 1$ und

$$\sum_{\omega \in \Omega} \Pr[\omega] = 1.$$

Eine Menge $E \subseteq \Omega$ heißt *Ereignis*. Die Wahrscheinlichkeit $\Pr[E]$ eines Ereignisses ist definiert durch

$$\Pr[E] := \sum_{\omega \in E} \Pr[\omega].$$

Ein diskreter Wahrscheinlichkeitsraum heißt *endlich*, falls $|\Omega| < \infty$.

Später: Kontinuierliche W'keitsräume ($\Omega = \mathbb{R}$)

Rechenregeln:

Für Ereignisse $A, B, A_1, A_2, \ldots$ gilt:

1. $\Pr[\emptyset] = 0, \Pr[\Omega] = 1$.
2. $0 \leq \Pr[A] \leq 1$.
3. $\Pr[\bar{A}] = 1 - \Pr[A]$.
4. Wenn $A \subseteq B$, so folgt $\Pr[A] \leq \Pr[B]$.
5. *(Additionssatz)* Wenn die Ereignisse $A_1, \ldots, A_n$ paarweise disjunkt sind (also wenn für alle Paare $i \neq j$ gilt, dass $A_i \cap A_j = \emptyset$), so folgt

$$\Pr\left[\bigcup_{i=1}^{n} A_i\right] = \sum_{i=1}^{n} \Pr[A_i].$$

Für eine unendliche Menge von disjunkten Ereignissen $A_1, A_2, \ldots$ gilt analog

$$\Pr\left[\bigcup_{i=1}^{\infty} A_i\right] = \sum_{i=1}^{\infty} \Pr[A_i].$$

Boolesche Ungleichung:

Für Ereignisse $A_1, \ldots, A_n$ gilt

$$\Pr\left[\bigcup_{i=1}^{n} A_i\right] \leq \sum_{i=1}^{n} \Pr[A_i].$$

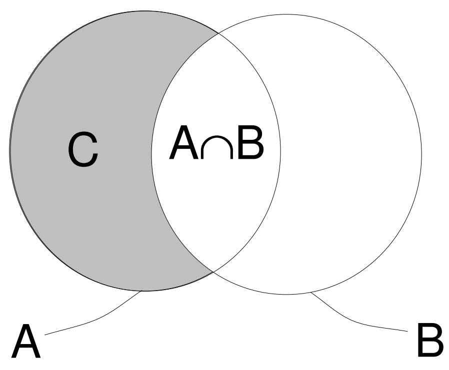
Analog gilt für eine unendliche Folge von Ereignissen $A_1, A_2, \ldots$, dass $\Pr\left[\bigcup_{i=1}^{\infty} A_i\right] \leq \sum_{i=1}^{\infty} \Pr[A_i]$.

Satz (Siebformel): Für beliebige Ereignisse $A_1, \ldots, A_n$ gilt:

$$\begin{aligned}\Pr[\bigcup_{i=1}^{n} A_i] &= \sum_{i=1}^{n} \Pr[A_i] - \sum_{1\le i_1<i_2\le n} \Pr[A_{i_1} \cap A_{i_2}] \\ &\quad + \sum_{1\le i_1<i_2<i_3\le n} \Pr[A_{i_1} \cap A_{i_2} \cap A_{i_3}] \\ &\quad - + \ldots + (-1)^{n-1}\Pr[A_1 \cap A_2 \cap \ldots \cap A_n]\end{aligned}$$

Beweisidee: Prinzip der Inklusion und Exklusion

Beweis ($n = 2$):
Setze $A := A_1$, $B := A_2$ und $C := A \setminus (A \cap B)$.



Dann sind C und $A \cap B$ disjunkt und analog C und B.
Nach dem Additionssatz (Rechenregel 5) gilt daher:

$$\Pr[\underbrace{C \cup (A \cap B)}_{= A}] = \Pr[C] + \Pr[A \cap B] \quad \text{und}$$

$$\begin{aligned}\Pr[\underbrace{C \cup B}_{= A\cup B}] &= \Pr[C] + \Pr[B] \\ &= \Pr[A] - \Pr[A \cap B] + \Pr[B].\end{aligned}$$

Prinzip von Laplace: *Wenn nichts dagegen spricht, gehen wir davon aus, dass alle Elementarereignisse gleich wahrscheinlich sind.*

Bei der Anwendung des Prinzips von Laplace gilt für alle Elementarereignisse $\Pr[\omega] = 1/|\Omega|$. Daraus erhalten wir für ein beliebiges Ereignis E die aus dem Schulunterricht bekannte Formel

$$\Pr[E] = \frac{|E|}{|\Omega|}.$$