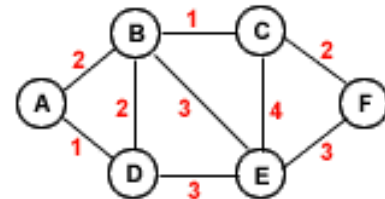




# Effiziente Algorithmen

Hartmut Klauck  
Universität Frankfurt  
SS 06

4.5.





# Boolesche Matrixmultiplikation mit Zeugen

- Gegeben seien Boolesche Matrizen  $A, B$
- $P=AB$  unter Boolescher Multiplikation
  
- Ein Zeuge für  $P[i,j]=1$  ist ein Index  $k$  mit  $A[i,k]=B[k,j]=1$
- Eine Zeugenmatrix sei eine Matrix, die an allen  $i,j$  mit  $P[i,j]=1$  einen Zeugen enthält, sonst 0
- Bestimme Zeugenmatrix!
- Beachte: Integermatrixmultiplikation liefert Anzahl der Zeugen



# Boolesche Matrixmultiplikation mit Zeugen

- Betrachte zuerst den Fall, dass es für jeden Eintrag von  $P$  nur höchstens einen Zeugen gibt.
- Setze  $A'[i,k]=k \cdot A[i,k]$  und multipliziere  $A'$  mit  $B$  durch Integermatrixmultiplikation
- Ergebnis:  $k$  mit  $A[ik]B[kj]=1$ , wenn es existiert
- Natürlich funktioniert dies nicht allgemein



# Boolesche Matrixmultiplikation mit Zeugen

- Unser Ansatz wird es sein, durch Randomisierung zu erreichen, dass mit hoher Wahrscheinlichkeit nur ein Zeuge vorhanden ist.



# Ansatz:

- Isoliere Zeugen
- Sei  $P[i,j]$  ein Eintrag mit  $w$  Zeugen.
- Wir kennen  $w$  nach einer Integermatrixmultiplikation
- Sei  $w \geq 2$
- Setze  $r$ , so dass  $n/2 \leq wr \leq n$
- **Behauptung:** eine zufällige Menge  $R \subseteq \{1, \dots, n\}$  mit  $|R|=r$  enthält mit guter Wahrscheinlichkeit genau einen Zeugen



# Zur Behauptung

- Veranschauliche als Spiel:
  - Es gebe  $n$  Bälle mit den Zahlen  $1 \dots n$
  - Davon seien  $w$  Bälle weiss, der Rest schwarz
  - Ziehe  $r$  Bälle zufällig ohne Zurücklegen
  - Wie gross ist die Wahrscheinlichkeit, genau einen weissen Ball zu haben?



# Lemma

- Die Wahrscheinlichkeit, genau einen weissen Ball zu sehen ist mindestens  $(1/2e)$
- Beweis:
  - Diese Wahrscheinlichkeit ist gleich:

$$\binom{w}{1} \cdot \binom{n-w}{r-1} / \binom{n}{r}$$

# Beweis:

$$\binom{w}{1} \cdot \binom{n-w}{r-1} / \binom{n}{r} = w \cdot \frac{r!}{(r-1)!} \frac{(n-w)!}{n!} \frac{(n-r)!}{(n-w-r+1)!}$$

$$= w \cdot r \left( \prod_{i=0}^{w-1} \frac{1}{n-i} \right) \left( \prod_{j=0}^{w-2} (n-r-j) \right)$$

$$= \frac{wr}{n} \prod_{j=0}^{w-2} \frac{n-r-j}{n-j}$$

$$\geq \frac{wr}{n} \prod_{j=0}^{w-2} \frac{n-r-j - (w-j-1)}{n-1-j - (w-j-1)}$$

$$= \frac{w \cdot r}{n} \prod_{j=0}^{w-2} \frac{n-w-(r-1)}{n-w}$$

• • • | Beweis:

$$= \frac{wr}{n} \left(1 - \frac{r-1}{n-w}\right)^{w-1}$$

$$\geq \frac{1}{2} \cdot \left(1 - \frac{1}{w}\right)^{w-1} \quad ; \quad \frac{n}{2} \leq wr \leq n$$

$$\geq \frac{1}{2} \cdot \frac{1}{e}$$



# Anwendung

- Wenn die Menge  $R$  genau einen Zeugen enthält, kann dieser leicht gefunden werden:
  - Sei  $R$  dargestellt durch einen Inzidenzvektor:  $R[k]=1$  gdw  $k \in R$
  - Setze  $A^R[i,k]=kR[k]A[i,k]$
  - Setze  $B^R[k,j]=R[k]B[k,j]$
  - Dann ist für alle  $i,j$  mit eindeutigem Zeugen  $A^R B^R[i,j]=k$  für den Zeugen  $k$
  - Insgesamt erhalten wir mit  $A^R B^R$  Zeugen für einen Bruchteil von  $1/(2e)$  aller Einträge für die  $r$  korrekt gewählt ist, d.h.  $n/2 \leq wr \leq n$
  - Zusätzlich ist es einfach, die Anzahl der Zeugen pro Eintrag zu berechnen, also können wir die Menge der korrekt bestimmten Zeugen identifizieren.
  - Wiederhole dies, bis für fast alle Einträge ein Zeuge gefunden



# Der Algorithmus

- Eingabe: Boolesche Matrizen  $A, B$
  - Ausgabe: Zeugenmatrix  $W$  für Boolesches Produkt  $AB$
1. Setze  $W = -AB$  (mit Integermatrixmult.)
  2. Von  $t=0$  bis  $\log n$ :
    - a)  $r = 2^t$
    - b) Wiederhole  $5 \log n$  mal:
      - i. Wähle  $R \subseteq \{1, \dots, n\}$  mit  $|R|=r$  zufällig
      - ii. Berechne  $A^R$  und  $B^R$
      - iii. Setze  $Z = A^R B^R$  (mit Integermatrixmult.)
      - iv. Für alle  $(i, j)$ : wenn  $W[i, j] < 0$  und  $Z[i, j]$  ist Zeuge dann  $W[i, j] = Z[i, j]$
  3. Für alle  $(i, j)$ : wenn  $W[i, j] < 0$ : finde Zeugen mit trivialer Methode



# Korrektheit

- ist klar nach vorheriger Diskussion.  
Insbesondere werden Zeugen immer nur korrekt gesetzt



# Laufzeit

- **Behauptung:** Erwartete Laufzeit ist nur  $O(T(n) \log^2 n)$ , wenn  $T(n)$  Laufzeit für Integermatrixmultiplikation ist.
- **Beweis:**
  - Klar: Bis (exklusive) Schritt 3 gilt Schranke
  - Schritt 3 braucht  $O(n)$  Zeit pro  $(i,j)$ , für welches noch kein Zeuge gefunden ist.
  - Noch zu zeigen: Wahrscheinlichkeit, dass Schritt 3 ausgeführt wird ist höchstens  $1/n$  für jedes  $i,j$ ; dann ist die erwartete Zeit für Schritt 3 nur  $n^2 \cdot 1/n \cdot O(n) = O(n^2)$ .  
[Anzahl der Matrixeinträge mal Wahrscheinlichkeit in Schritt 3 erst Zeugen zu finden mal Laufzeit für brute force Zeugensuche]



# Laufzeit

- Betrachte eine Eintrag  $[i, j]$  mit  $\geq 2$  Zeugen
- In Schleife 2 wird irgendwann ein  $r$  mit  $n/2 \leq wr \leq n$  gewählt
- Die Wahrscheinlichkeit, einen einzigen Zeugen zu bestimmen ist dann  $1/(2e)$  pro Durchlauf von Schleife b)
- Wahrscheinlichkeit, dass dies nie geschieht ist daher  $(1 - 1/(2e))^{\log n} < 1/n$