05.04.
2018

Wahrscheinlichkeitsrechnung und Algorithmik

Sommersemester 2018

1. Unabhängige Menge

(Wilf: „Algorithms and Complexity")

Graph $G = (V, E)$ ungerichteter Graph,
(übliche Definition)

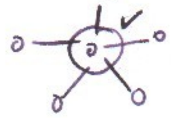
$I \subseteq V$ ist unabhängige Menge.
$\Leftrightarrow$
Es gibt keine Kante $\{v, w\} \in E$ mit $v, w \in I$.

~

Maximale unabh. Menge $\Leftrightarrow$ Jeder weitere Knoten verletzt Unabhängigkeit d. Menge

◦ Finden einer maximalen unabhängigen Menge.

1. Wähle beliebigen Knoten v
   - Entferne alle Nachbarn von v aus dem Graphen
     D.h. alle Knoten w mit $\{v, w\} \in E$

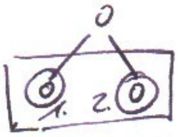


2. Wähle einen Knoten aus dem Rest, solange der Rest Knoten hat. Gehe analog zu 1 vor. ↺ usw.

Ausgabe: Menge der gewählten Knoten.

⇒ Findet nicht das Maximum aller unabhängigen Mengen!

z.B.  ⇒ Ecke, Größe 1

 ⇒ Größe 2

∘ Finden des Maximums ist NP-vollständig!

dazu: Erfüllbarkeitsproblem 3-SAT
(Reduktion 3-SAT $\leq_p$ unabh. Menge)

gegeben: Aussagenlog. Formel der Art

$$\overbrace{(x_1 \vee x_2 \vee x_7)}^{\leq 3} \wedge \ldots$$

1/0
wahr/falsch

n Variablen, 2^n potentielle Lösungen

Vermutung: 3-SAT nicht in Polynomialzeit lösbar. NP vollständig

gesucht: Werte für Variablen, so dass Formel zu ~~0~~ 1 auswertet.

05.04.2018

Einschub: $2^n > n^c$

1. $2^n \geq n+1$ für alle $n \geq 0$, einfache Induktion
2. Es folgt

   $2^{n-1} \geq n$ für alle $n \geq 1$ (Substitution)

3. Es folgt

   $2^n \geq 2n$ für alle $n \geq 1$

4. Es folgt

   $2^{\frac{1}{2}n} \geq n$ für alle $n \geq 2$ (Substitution)

5. Es folgt

   $2^n \geq n^2$ f. alle $n \geq 2$

   ↑ f. $c=2$

   ↙ für beliebiges c

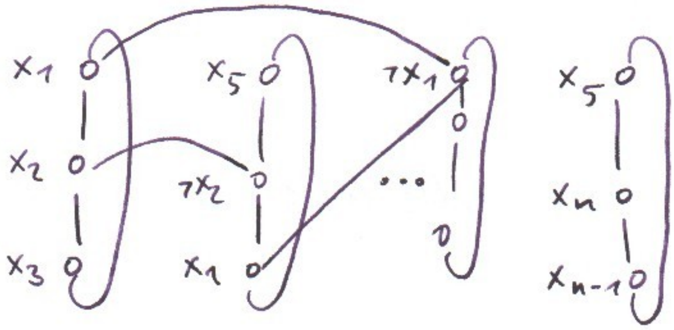
1. $2^n \geq n$
2. $2^{c \cdot n} \geq n^c$
3. $2^n \geq \left(\frac{n}{c}\right)^c = \left(\frac{1}{c}\right)^c \cdot n^c = \left(\frac{1}{c}\right)^c \cdot n^\varepsilon \cdot n^{c-\varepsilon} \geq n^{c-\varepsilon}$

Übersetzung von 3-SAT $\rightsquigarrow$ Das Maximum der unabhängigen Mengen finden.

<u>Bsp.</u>: $(\underbrace{x_1}_{=1} \vee x_2 \vee \neg x_3) \wedge (x_5 \vee \neg x_2 \vee \underbrace{x_1}_{=1}) \wedge \ldots \wedge (\underbrace{x_5}_{=1} \vee x_n \vee \neg x_{n-1})$

- Variablen $x_1 \ldots x_n$
- m Klauseln

für jeden Platz in den Klauseln einen Knoten.



(#Knoten = #Positionen der Formel)

Lösbarkeit $\hat{=}$ Existenz eines widerspruchsfreien Weges durch die Klauseln

($(x_1 \vee x_2) \wedge (\neg x_1) \wedge (\neg x_2)$ hat <u>keinen</u> widerspruchsfreien Weg!)

$\Rightarrow$ alles, was nicht zum Weg gehört, mit Kanten verbinden

$\Rightarrow$ <u>alle</u> innerhalb einer Klausel

$\Rightarrow$ <u>alle</u> zwischen Klauseln wo sich die Variablen widersprechen, d.h. Kanten zwischen

$x_i, \neg x_i$

<u>Jetzt gilt</u>: Formel erfüllbar $\Longleftrightarrow$ Graph enthält maximale unabhängige Menge der Größe m

(Und das Maximum ist m.)

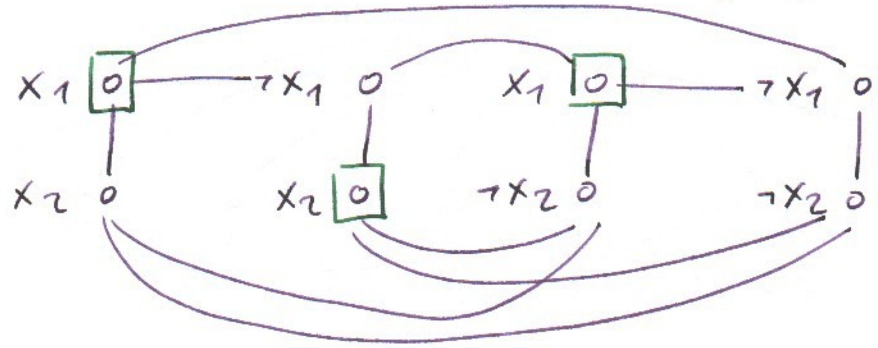
05.04.
2018

Verdeutlichung am Beispiel:

$$(x_1 \vee x_2) \wedge (\neg x_1 \vee x_2) \wedge (x_1 \vee \neg x_2) \wedge (\neg x_1 \vee \neg x_2)$$

$$(0 \quad 0) \quad (1 \quad 0) \quad (0 \quad 1) \quad (1 \quad 1)$$

Klausel falsch bei dieser Belegung.

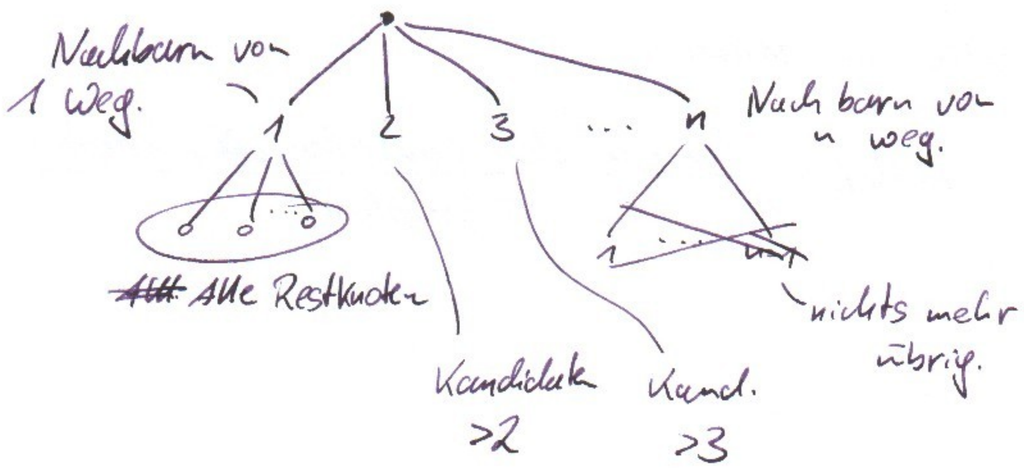


Größte unabh. Menge ist 3. ⇒ Unerfüllbar.

(Übung: Konstruktion an kleinem Beispiel)

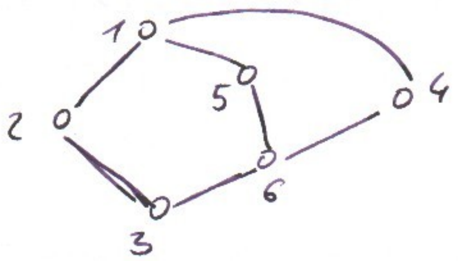
Algorithmus für Maximum der unabh. Mengen.

⇒ Backtracking über Knoten (rekursives Aufzählen der Lösungskandidaten Knoten $V = \{1, \dots, n\}$)

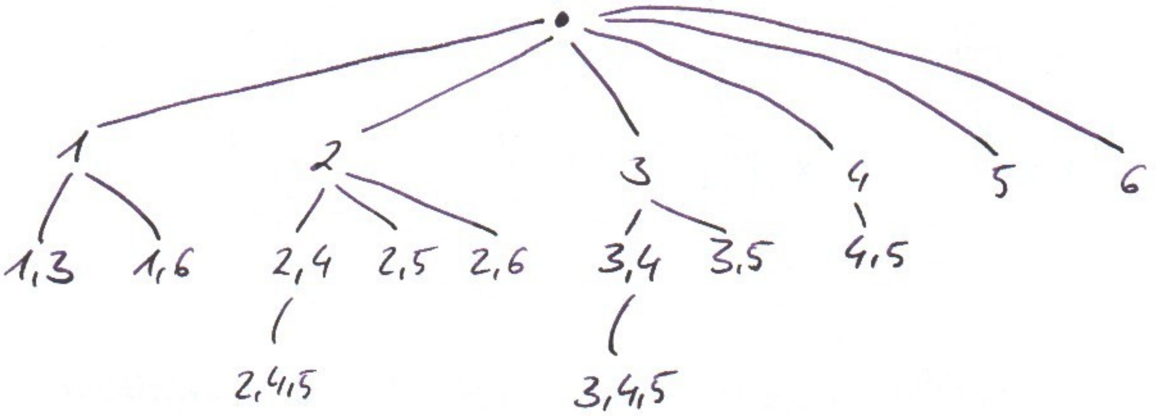


⇒ Jede unabhängige Menge wird genau einmal generiert.

<u>Beispiel:</u>



BT-Baum:



~~Pro Knoten im~~

Pro unabhängige Menge ein Knoten im Baum.

- Keine Kante im ~~Graft~~ Graph $\Leftrightarrow$ 2^n Knoten im Baum
- Alle möglichen Kanten in G $\Leftrightarrow$ n Knoten im Baum

$\Rightarrow$ worst-case $\geq 2^n$ (bei n Knoten)

↳ Wie im Mittel?

$$\text{Mittel} = \frac{\text{Summe der Laufzeiten aller Graphen}}{\#\ \text{Graphen}}$$

05.04.2018

$\# \text{Graphen} = 2^{\binom{n}{2}}$

Knotenmenge $V = \{1, \dots, n\}$

$\binom{n}{2} = \#$ möglicher Kanten

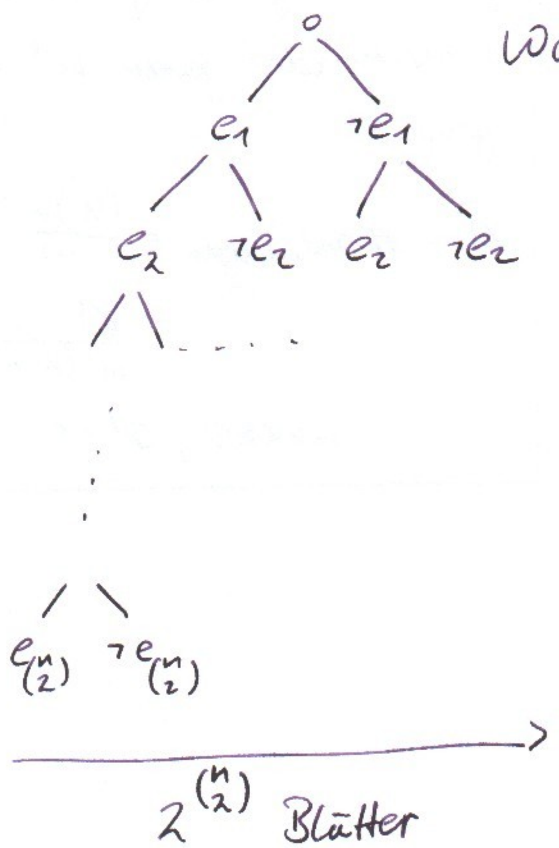
$\binom{n}{2} = \frac{n(n-1)}{2}$ $\qquad 2^{\binom{n}{2}} = \sqrt{2}^{\,n(n-1)}$

<u>Wahrscheinlichkeitsraum der Graphen auf $V = \{1, \dots, n\}$</u>

$\text{Prob}[G] = \frac{1}{2^{\binom{n}{2}}}$ uniforme Verteilung.

Graphen <u>generieren:</u>

- Mögliche Kanten $e_1, \dots, e_{\binom{n}{2}}$ irgendwie angeordnet
- Wahrscheinlichkeitsbaum



Wahrscheinlichkeiten jeweils $\frac{1}{2}$

Unabhängig $\Rightarrow$ Multiplikation

Prob[$\mathcal{G}$; $\mathcal{G}$ hat genau m Kanten]

$$\overset{\#}{=} \frac{\binom{\binom{n}{2}}{m}}{2^{\binom{n}{2}}} < 1$$

Typische # Kanten $\approx \frac{\binom{n}{2}}{2}$

- K Elemente insgesamt $1, \dots, K$
- # Teilmengen mit genau m Elementen

Geordnete m-Tupel, wobei alle Elemente verschieden.

$= K \cdot (K-1) \cdot \ldots \cdot (K-m+1)$

$=: (K)_m$

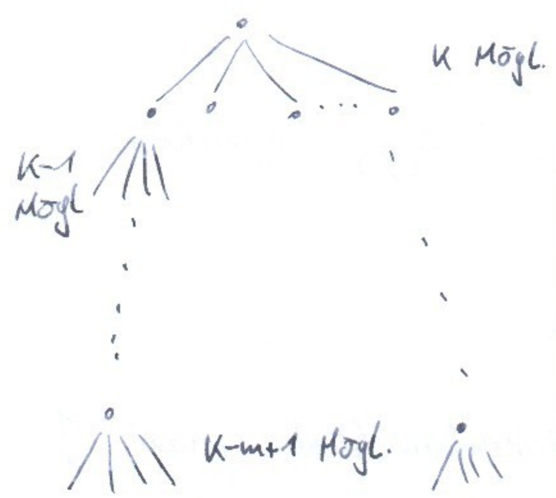
Jede Teilmenge mit genau m Elementen wird genau m! mal generiert

Also # Teilmengen $= \frac{(K)_m}{m!}$

$$= \frac{K!}{m!\,(K-m)!} = \binom{K}{m}$$

$m \geq K \geq 0$, $0! = 1$

als Baum:



Jede Menge m! mal!

12.04.
2018

- <u>Zufallsvariable</u> $X : \begin{pmatrix} \text{Menge der Graphen auf} \\ \text{Knoten } \{1, \dots, n\} \end{pmatrix} \to \mathbb{R}$

<u>z. B.</u>: $X(G) = \#\text{Kanten von } G$.

$$\text{Prob}[X(G) = m] := \text{Prob}[G ; X(G) = m]$$
$$= \text{Prob}[X^{-1}(m)]$$

- Zufallsvariable Y ist <u>binomialverteilt</u> mit Parameter K, p, $0 < p < 1$

bedeutet: $\text{Prob}[Y = m] = \binom{K}{m} \cdot p^m \cdot (1-p)^{K-m}$ für $0 \leq m \leq K$

($\Rightarrow$ d.h. $\text{Prob}[G ; G$ hat genau m Kanten$]$ ist binomialverteilt mit $K = \binom{n}{2}$, $p = \frac{1}{2}$)

- Z irgendeine Zufallsvariable, Erwartungswert $E[Z]$:

$$E[Z] = \sum_{\omega \in \Omega} \text{Prob}[\omega] \cdot Z(\omega)$$

Ω Ursprungsraum, endlich

$$= \sum_{m} \text{Prob}[Z = m] \cdot m$$

Beispiel: Würfel $\quad Z(\omega) = \omega \quad \omega \in \{1, 2, 3, 4, 5, 6\}$

$$\mathrm{Prob}[\omega] = \frac{1}{6}$$

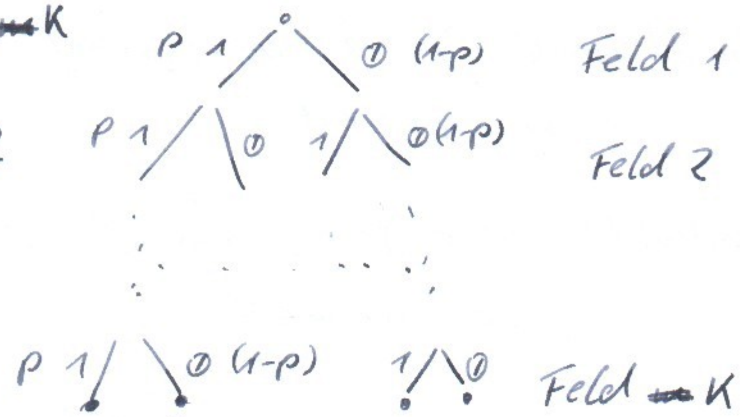
$$E[Z] = 3{,}5$$

Erwartungswert von Y oben: (~~Ewer~~ E-wert einer binomialverteilten Zufallsvar.)

- Veranschaulichung durch einen geeigneten Raum:

Felder: $1, \dots, K$

Raum: $\{0, 1\}^K = \Omega$



$$\mathrm{Prob} = p^{\#\text{Einsen}} \cdot (1-p)^{\#\text{Nullen}}$$

$Y = \#$ Einsen in der Folge

$$\mathrm{Prob}[Y = m] = \binom{K}{m} \cdot p^m \cdot (1-p)^{K-m}$$

↳ binomialverteilt

$$\boxed{E[Y] = p \cdot K}$$

Bsp: $\quad E[Y]$

$p = 0 \Rightarrow 0$

$p = 1 \Rightarrow K$

$p = \frac{1}{2} \Rightarrow \frac{K}{2}$

12.04.
2018

<u>Beweis:</u>

$$E[Y] = \sum_{m=0}^{K} \underbrace{\binom{K}{m} p^m (1-p)^{K-m}}_{Prob[Y=m]} \cdot m$$

$$= \sum_{m=1}^{K} m \cdot \frac{K!}{m!\,(K-m)!}\, p^m (1-p)^{K-m}$$

$$= \sum_{m=1}^{K} \frac{K!}{(m-1)!\,(K-m)!}\, p^m (1-p)^{K-m}$$

$$= \sum_{m=1}^{K} \frac{K\,(K-1)!}{(m-1)!\,((K-1)-(m-1))!} \cdot p^m (1-p)^{(K-1)-(m-1)}$$

$$= K \cdot p \cdot \sum_{m=1}^{K} \frac{(K-1)!}{\underbrace{(m-1)}_{\text{0 bis } K-1}!\,((K-1)-(m-1))!}\, p^{m-1} (1-p)^{(K-1)-(m-1)}$$

$$= K \cdot p \cdot \sum_{l=0}^{K-1} \frac{(K-1)!}{l!\,((K-1)-l)!}\, p^l (1-p)^{(K-1)-l}$$

$$= K \cdot p \cdot \underbrace{\sum_{l=0}^{K-1} \underbrace{\binom{K-1}{l} p^l (1-p)^{(K-1)-l}}_{Prob[\hat{Y}=l]}}_{=1}$$

$\left(\hat{Y}\right.$ mit $K-1, p$ binomial verteilt$\left.\right)$

Einfacher mit Linearität des Erwartungswertes:

X, Y Zufallsvar.

$X: \Omega \to \mathbb{R}$

$Y: \Omega \to \mathbb{R}$

gleicher Raum

$(X+Y): \Omega \to \mathbb{R}$

$(X+Y)(\omega) := X(\omega) + Y(\omega)$

Linearität:

$\Rightarrow$ $E[X+Y] = E[X] + E[Y]$ (Beweis: Übung)

Zerlege Y in einzelne Y_i mit

$$Y_i(b_1, b_2, \ldots, b_k) = \begin{cases} 1 & \text{wenn } b_i = 1 \\ 0 & \text{wenn } b_i = 0 \end{cases} \quad \text{Indikator ZV}$$

$$Y = Y_1 + Y_2 + \ldots + Y_k$$

$$E[Y] = E[Y_1 + \ldots + Y_k] = E[Y_1] + E[Y_2] + \ldots + E[Y_k]$$

$$E[Y_1] = 1 \cdot \mathrm{Prob}[Y_1 = 1] + 0 \cdot \mathrm{Prob}[Y_1 = 0]$$

$$= \mathrm{Prob}[Y_1 = 1] = p$$

für alle anderen Y_i auch!

$$\Rightarrow E[Y] = k \cdot p$$

12.04.
2018

Für den Graphen von oben:

$X := \#$ Kanten in G

$E[X] = \frac{1}{2} \cdot \binom{n}{2}$ (1 ≙ Kante dabei, 0 ≙ nicht)

⇒ Erwartungswert alleine sagt noch nicht viel:

$\Omega = \{(\underbrace{00 \ldots 0}_{k \text{ Stück}}), (\underbrace{11 \ldots 1}_{k \text{ Stück}})\}$ Wkt $= \frac{1}{2}$

$Y = \#$ Einsen, $\underbrace{E[Y] = k \cdot \frac{1}{2}}$

weit weg von tatsächlich auftretenden Werten von Y!

Erwartungswert und Konkretes zufällig generiertes Element.

Satz: Ist $Y \geq 0$ eine Zufallsvariable, dann für alle $a \gneq 0$:

$$\text{Prob}[Y \geq a] \leq \frac{E[Y]}{a}.$$

(Sinnvoll nur bei $a \gneq E[Y]$.)

Beweis: $E[Y] = a_1 \cdot \text{Prob}[Y = a_1] + a_2 \cdot \text{Prob}[Y = a_2] + \ldots + \ldots + a_l \cdot \text{Prob}[Y = a_l]$

$a_1 \leq a_2 \leq \ldots \leq a_l$

$= a_1 \cdot \text{Prob}[Y = a_1] + \ldots + \overbrace{a_h}^{\leq a} \text{Prob}[Y = a_h]$

$+ \underbrace{a_{h+1}}_{\geq a} \text{Prob}[Y = a_{h+1}] + \ldots + a_l \text{Prob}[Y = a_l]$

$$E[Y] = \overbrace{a_1 \, Prob[Y=a_1] + \ldots + \underbrace{a_h}_{\le a} \cdot Prob[Y=a_h]}^{\ge 0}$$

$$+ \underbrace{a_{h+1}}_{\ge a} Prob[Y=a_{h+1}] + \ldots + \underbrace{a_L}_{\ge a} Prob[Y=a_L]$$

$$\ge 0 + a \cdot Prob[Y \ge a]$$

$$\Rightarrow E[Y] \ge a \cdot Prob[Y \ge a]$$

$$\Leftrightarrow Prob[Y \ge a] \le \frac{E[Y]}{a}$$

$\blacksquare$

Bsp: ∘ Binomial $k, \frac{1}{2}$ verteilte ZV Y

E-Wert: $\frac{1}{2} k$

$$Prob[Y \ge \tfrac{3}{4} k] \le \frac{\frac{1}{2} k}{\frac{3}{4} k} = \frac{2}{3}$$

∘ Raum Ω $((0 \_ 0), (1 \_ 1))$

$Y = \#$ Einsen

$$Prob[Y \ge \tfrac{3}{4} k] \le \frac{2}{3}.$$

12.04.2018

Z irgendeine Zufallsvariable.

<u>Neue ZV</u>: $(Z-E[Z])^2 \rightsquigarrow ZV \geq 0$, <u>Varianz</u>

$$(Z-E[Z])^2(\omega) = (Z-E[Z])(\omega)\cdot(Z-E[Z])\omega$$
$$= (Z(\omega)-E[Z])\cdot(Z(\omega)-E[Z])$$
$$= \underline{\underline{(Z(\omega)-E[Z])^2}}$$

19.04.2018

$Prob(Y \geq a) \leq \frac{E[Y]}{a}$ (Markov)

Anwendung auf die Abweichung von Y vom Erwartungswert $E[Y]$.

$(Y-E[Y])$ nicht sinnvoll $E[Y-E[Y]] = E[Y]-E[Y]$

$(Y-E[Y])^2 \geq 0$ besser!

$(Y-E[Y])^2(\omega) = (Y(\omega)-E[Y])^2 \geq 0$

↳ aus dem Raum von Y

$$\boxed{E[(Y-E[Y])^2]}$$
$$= E[Y^2 - 2Y\,E[Y] + (E[Y])^2]$$
$$= E[Y^2] - 2(E[Y])^2 + (E[Y])^2$$
$$\boxed{= E[Y^2] - (E[Y])^2} = Var[Y] \geq 0 \Leftrightarrow E[Y^2] \geq (E[Y])^2$$

↳ Varianz

Markov-Ungleichung für $(Y-E[Y])^2$

$$\text{Prob}\left[(Y-E[Y])^2 \geq a\right] \leq \frac{E[Y^2]-(E[Y])^2}{a}$$

$$= \frac{Var[Y]}{a}$$

<u>Anwendung, wenn Y der Binomialverteilung mit m, b folgt?</u>

Dazu $(E[Y])^2 = (p\cdot m)^2$

$$E[Y^2] = \sum_{K=0}^{m}\left(K^2 \cdot \underbrace{\binom{m}{K} p^K (1-p)^{m-K}}_{\text{Prob}[Y=K]}\right)$$

$$Y = Y_1 + Y_2 + \ldots + Y_m \qquad Y(b_1 \text{–} b_m) = \overbrace{Y_1(b_1 \text{–} b_m)}^{=b_1} + \ldots + \underbrace{Y_m(b_1 \text{–} b_m)}_{=b_m},$$

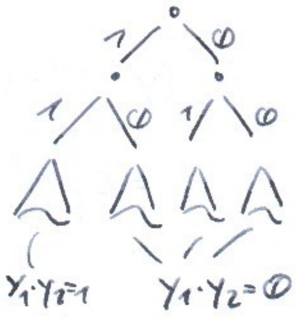
$$Y^2 = (Y_1 + \ldots + Y_m)(Y_1 + \ldots + Y_m)$$

$$= \sum_{i=1}^{m} \underbrace{Y_i^2}_{=Y_i} + \sum_{i=1}^{m} \sum_{\substack{j=1 \\ j\neq i}}^{m} (Y_i \cdot Y_j)$$

$$E[Y^2] = E[Y] + \sum_{i=1}^{m} \sum_{\substack{j=1 \\ j\neq i}}^{m} \underbrace{E[\overset{Y_i \cdot Y_j}{\cancel{X_i \cdot X_j}}]}_{=p^2}$$

$$= \cancel{m\cdot p + m(m-1)\cdot p^2}$$

$$= m\cdot p + m(m-1)\cdot p^2$$



$$\text{Prob}[Y_1 \cdot Y_2 = 1] = p^2$$

$$= E[Y_1 \cdot Y_2]$$

19.04.
2018

$m \cdot p + m(m-1)p^2$

$= E[Y] + m^2p^2 - mp^2$

$= E[Y] + (E[Y])^2 - mp^2$

$\boxed{Var[Y]} = E[Y^2] - (E[Y])^2$

$= p \cdot m + \cancel{m^2p^2} - mp^2 - \cancel{m^2p^2}$

$= \boxed{mp(1-p)} = E[Y] \cdot (1-p)$

<u>Was ist $p(1-p)$?</u> Das ist $V[Y_i]$.

$V[Y_i] = E[Y_i^2] - (E[Y_i])^2$

$= p - p^2 = p(1-p)$

$Prob[(Y - E[Y])^2 \geq a] \leq \frac{Var[Y]}{a}$ für alle ZV Y.

Y binomial mit m, p dann rechte Seite:

$\frac{V[Y]}{a} = \frac{mp(1-p)}{a} = \frac{1}{c}$ für

(p Konstant, m groß)

$a = c \cdot mp(1-p)$

$$\mathrm{Prob}\left[\,|Y-E[Y]| \geq \sqrt{c\cdot m\cdot p(1-p)}\,\right]$$

$$= \mathrm{Prob}\left[(Y-E[Y])^2 \geq c\cdot m\cdot p\cdot(1-p)\right] \leq \frac{1}{c}$$

$$\mathrm{Prob}\left[\,|Y-E[Y]| \geq \sqrt{c\cdot m\cdot p}\,\right]$$

$$\leq \mathrm{Prob}\left[\,|Y-E[Y]| \geq \sqrt{c\cdot m\cdot p\cdot(1-p)}\,\right] \leq \frac{1}{c}$$

$$\mathrm{Prob}\left[\,|Y-E[Y]| \geq (1+\varepsilon)\cancel{\sqrt{E[X]}}\sqrt{E[Y]}\,\right]$$

$$\leq \mathrm{Prob}\left[(Y-E[Y])^2 \geq (1+\varepsilon)^2\,\cancel{E[X]}\,E[Y]\right]$$

$$\mathrm{Prob}\left[(Y-E[Y])^2 \geq a\right] \leq \frac{E[Y^2]-(E[Y])^2}{a}$$

$$= \frac{mp - mp^2}{a}$$

$$a = (\varepsilon\cdot m\cdot p)^2$$

$$\mathrm{Prob}\left[(Y-E[Y])^2 \geq (\varepsilon\cdot m\cdot p)^2\right] \leq \frac{mp-mp^2}{\varepsilon^2 m^2 p^2}$$

$$= \frac{1-p}{\varepsilon^2 mp} \to 0$$

$$= \mathrm{Prob}\left[\,|Y-E[Y]| \geq \varepsilon\cdot m\cdot p\right]$$

m groß,
p, ε Konst.

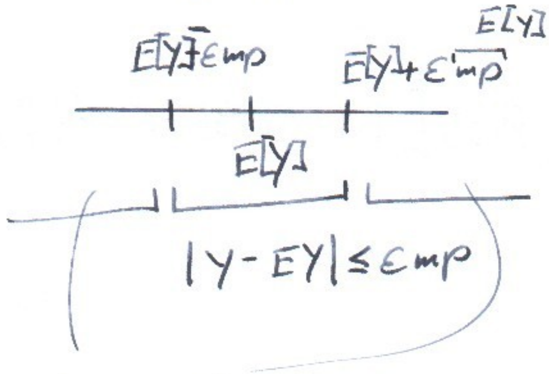
Das heißt $\mathrm{Prob}[Y \leq E[Y] + \varepsilon\cdot mp$
oder
$Y \geq E[Y] - \varepsilon\cdot mp] = 1 - \frac{1-p}{\varepsilon^2 mp} \to 1$

$$|Y - E[Y]| \ge \varepsilon mp \Leftrightarrow Y - E[Y] \ge \varepsilon mp$$

oder

$\cancel{Y - E[Y]}$

$$E[Y] - Y \ge \varepsilon mp$$



$$|Y - E[Y]| \ge \varepsilon mp.$$

$$\text{Prob}\left[|Y - E[Y]| \ge \varepsilon mp\right] = \frac{1-p}{\varepsilon^2 mp}$$

$$\Rightarrow \text{Prob}\left[Y \ge (1-\varepsilon)E[Y] \text{ und } Y \le (1+\varepsilon)E[Y]\right]$$

$$= 1 - \frac{1-p}{\varepsilon^2 mp} \to 1$$

(Chebyscheff-Ungleichung / Gesetz der großen Zahlen)

Zufällige Graphen:

$X(G) = \#$ Kanten in G.

Mit Wahrscheinlichkeit $\to 1$ liegt X bei

$$\frac{1}{2} \cdot \binom{n}{2} = \frac{1}{4} \cdot n(n-1)$$

$$\text{Prob}\left[\,|X - E[X]| \geq \varepsilon \cdot \frac{1}{2}\binom{n}{2}\right] \leq \frac{1}{\varepsilon^2 \binom{n}{2}}$$

$\leadsto$  fester ~~jeder~~ Knoten im Graph hat etwa $\frac{n}{2}$ Nachbarn.

$\Big($ $X_1 = \#$ Nachbarn von 1

X_1 verteilt nach binomial mit $n-1$, $\frac{1}{2}$ $\Big)$

$$\text{Prob}[\text{Knoten } x \text{ ohne Nachbarn}] = \left(\frac{1}{2}\right)^{n-1}$$

Prob[Knoten 1 od. 2 od. ... od. n ohne Nachbarn]

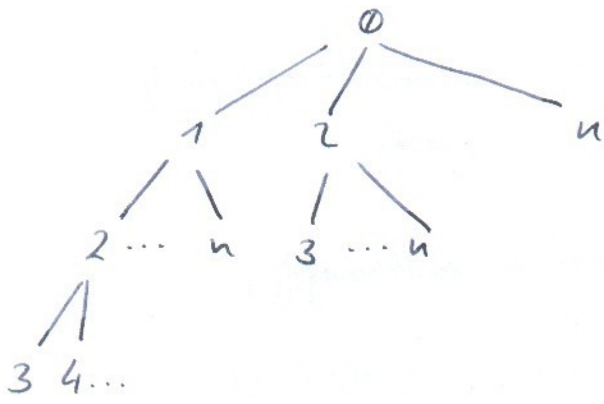
$\leq$ Prob[1 ohne N.] + ... +

Prob[n ohne N.]

$= \left(\frac{1}{2}\right)^n + \ldots + \left(\frac{1}{2}\right)^n = n \cdot \left(\frac{1}{2}\right)^n \to 0$

$\Big[$ $\text{Prob}[A \cup B] =$
$\text{Prob}[A] +$
$\text{Prob}[B] -$
$\text{Prob}[A \cap B]$

Laufzeit für Backtracking-Algorithmus f. Unabhängige Menge.



$\leq 2^n$ Knoten
(für jede Teilmenge von $\{1, \ldots, n\}$ ein Knoten im Baum, wenn der Graph das zuläßt)

Anwendung auf G:

Knoten im Baum $\hat{=}$ unabhängige Mengen von G

$X(G) = \#$ Knoten im Baum zu G

$= \#$ unabhängige Mengen von G

($\hat{=}$ Laufzeit)

Was ist $E[X]$?

$\Rightarrow$ Darstellen als Summe von Indikatoren!

$$X = X_\emptyset + X_{\{1\}} + \ldots + X_S + \ldots + X_{\{1, \ldots, n\}}$$

$S \subseteq \{1, \ldots, n\}$

$$X_S = \begin{cases} 1 & S \text{ unabhängig in } G \\ 0 & S \text{ enthält Kante in } G \end{cases}$$

26.04.
2018

Indikatorvariablen

X_S für $S \subseteq \{1, \dots, n\}$

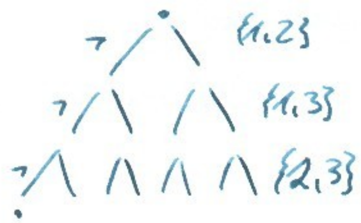
$$X_S(G) = \begin{cases} 1 & S \text{ unabhängig in } G \\ 0 & \text{sonst} \end{cases}$$

$$E[X_S] = \text{Prob}[S \text{ unabhängig}]$$

z.B. $S = \{1, 2, 3\}$

mögliche Kanten

$\{1,2\}$ $\{1,3\}$ $\{2,3\}$



$\left(\frac{1}{2}\right)^3$

Prob[$\{1,2,3\}$ unabh.]

bei k Knoten in S

$$\text{Prob}[S \text{ unabh.}] = \left(\frac{1}{2}\right)^{\binom{k}{2}}$$

$$X(G) = X_\emptyset(G) + X_{\{1\}}(G) + \dots + X_{\{v_1, v_2, \dots, v_k\}}(G) + \dots + X_{\{1, \dots, n\}}(G)$$

$\rightarrow 2^n$ Summanden.

$$\left(X(G) = \sum_{S \subseteq \{1, \dots, n\}} X_S(G) \right)$$

26.04.
2018

$$E[X] = \sum_{S \subseteq \{1,\dots,n\}} Prob[X_S = 1]$$

$$= \sum_{k=0}^{n} \binom{n}{k} \cdot \left(\frac{1}{2}\right)^{\binom{k}{2}}$$

Mittlere Laufzeit des Backtracking Algorithmus.

$\left(\frac{1}{2}\right)^{\binom{k}{2}}$ fällt extrem schnell in k.

$\binom{n}{k}$ steigt erstmal bis zu $\lfloor \frac{n}{2} \rfloor$, fällt dann wieder.

Was ergibt das?

Abkürzungen: $t_k := \binom{n}{k} \cdot \left(\frac{1}{2}\right)^{\binom{k}{2}} = \binom{n}{k} \cdot \sqrt{\left(\frac{1}{2}\right)^{k(k-1)}}$

$t_0 = 1$, $t_1 = n \cdot 1$, $t_2 \frac{n(n-1)}{2} \cdot \frac{1}{2}$, ...

$t_0 < t_1 < t_2$ für n groß genug.

$t_n = 1 \cdot \left(\frac{1}{2}\right)^{\binom{n}{2}}$ $\Rightarrow$ extrem klein!

Vermutung: $t_0 < t_1 < t_2 < \dots < t_{k_0} > t_{k_0+1} > \dots > t_n$

$\uparrow$ Das Maximum.

Ziel: $\sum_{i=0}^{n} t_i < (n+1) \cdot t_{k_0}$

Betrachten den Quotienten:

$$\frac{t_k}{t_{k-1}} > 1 \iff t_k > t_{k-1} \qquad k \geq 1$$

$$\frac{t_k}{t_{k-1}} < 1 \iff t_k < t_{k-1} \qquad k \geq 1$$

$$\frac{t_k}{t_{k-1}} = \frac{\binom{n}{k} 2^{\binom{k-1}{2}}}{\binom{n}{k-1} 2^{\binom{k}{2}}} = \frac{(n)_k \, (k-1)!}{k! \, (n)_{k-1}} \cdot 2^{-\left(\binom{k}{2} - \binom{k-1}{2}\right)}$$

$$= \underbrace{\frac{n-k+1}{k} \cdot \frac{1}{2^{k-1}}}_{\text{Streng monoton fallend in } k.}$$

$$\boxed{\left((n)_k = \frac{n!}{(n-k)!} \right)}$$

$\Rightarrow$ t_k haben tatsächlich nur ein Maximum!

Es gibt ein k_0 mit $t_0 < \ldots < \underbrace{t_{k_0} \geq t_{k_0+1}} > \ldots > t_n$

Welches k_0 ist dies? Wie ist der Wert von t_{k_0}?

26.01.
2018

- setzen $K = \lfloor \log_2 n \rfloor$, dann

$$\frac{t_K}{t_{K-1}} = \underbrace{\frac{n - \lfloor \log_2 n \rfloor + 1}{\lfloor \log_2 n \rfloor}}_{\approx \frac{n}{\log_2 n}} \cdot \underbrace{\left(\frac{1}{2}\right)^{\lfloor \log_2 n \rfloor - 1}}_{\gtrsim n} < 1$$

$\rightsquigarrow$ bei $K = \lfloor \log_2 n \rfloor$ bereits im fallenden Bereich der t_K.

$\rightsquigarrow$ $K_0 + 1 \leq \lfloor \log_2 n \rfloor$

- setzen $K = \lfloor \log_2 n - \log_2(\log_2 n) \rfloor$

$$\frac{t_K}{t_{K-1}} = \frac{n - \lfloor \log_2 n - \log_2(\log_2 n) \rfloor + 1}{\underbrace{\lfloor \log_2 n - \log_2(\log_2 n) \rfloor}_{< \log_2 n}} \cdot \underbrace{\left(\frac{1}{2}\right)^{\lfloor \log_2 n - \log_2(\log_2 n) \rfloor - 1}}_{\leq \frac{1}{2} \cdot \frac{n}{\log n}}$$

$\cancel{\geq}$ ~~$n - \log_2 n + 1$~~

$$\geq \frac{n - \lfloor \log_2 n - \log_2 \log_2 n \rfloor + 1}{\frac{n}{2}} = 2 - o(1) + o(1)$$

$o(1)$ = etwas, das gegen 0 geht.

$\to 2$, also > 1 für n groß genug.

$$t_0 < t_1 < \dots < t_{k_0} \geq t_{k_0+1} > \dots > t_n$$

$$\log_2 n - \log_2 \log_2 n < \underbrace{k_0 < \log_2 n}_{\text{Bereich für } k_0.}$$

t_k für $\lfloor \log_2 n - \log_2(\log_2 n) \rfloor \leq k_0 \leq \lfloor \log_2 n \rfloor$

Ziel: $t_k = \cancel{\mathcal{O}} \left(\cancel{n(n+\varepsilon)^{\log_2 n}} \right)$ für jedes $\varepsilon > 0$,
$= \mathcal{O}(n^{\log_2 n})$ sofern n groß genug ist.

$$t_k = \binom{n}{k} \frac{1}{2^{\binom{k}{2}}} \qquad k = \lfloor \log_2 n \rfloor$$

$$\frac{(n)_{\lfloor \log_2 n \rfloor}}{\lfloor \log_2 n \rfloor !} \cdot \frac{1}{2^{(\log_2 n)((\log_2 n)-1)\cdot \frac{1}{2}}}$$

$$\leq n^{\log_2 n}$$

$$k = \lfloor \log_2 n - \log_2(\log_2 n) \rfloor$$

$$\frac{(n)_{\lfloor \log_2 n - \log_2(\log_2 n) \rfloor}}{\lfloor \log_2 n - \log_2(\log_2 n) \rfloor !} \cdot \frac{1}{2^{(\log_2 n - \log\log n)(\dots - 1)\cdot \frac{1}{2}}}$$

$$\leq n^{\log_2 n}$$

- scheint für alle $k = \log_2 n - l$ für $l \leq \log \log n$ zu gelten.

26.04.2018

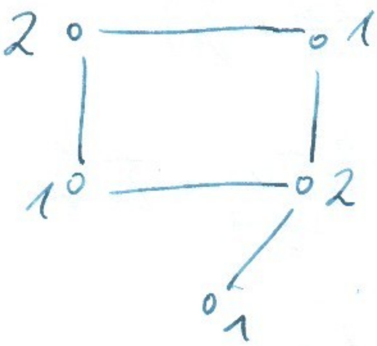
Also $E[X] \leq n \cdot n^{\log n} \leq n^{(1+\varepsilon)\log n}$

$$= (n+\varepsilon')^{\log n}$$

da $n < n^{\varepsilon \cdot \log_2 n}$

---

2. Graphfärbung

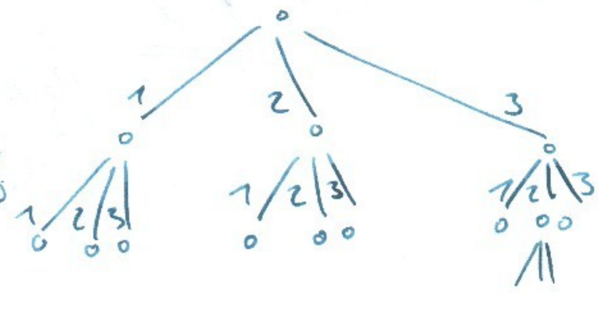


Frage:
Kommt man mit K Farben, K Konst. aus?

Prinzip: Nehme kleinste mögliche Farbe ~~(K=3)~~

(K=3)

je nachdem, welche Kanten da sind.



Knoten 1

Knoten 2

Knoten 3

⇝ Backtracking-Baum,

mittlere #Knoten im Baum?

$X(\mathcal{G}) = \#$ Knoten im Baum von $\mathcal{G}$.

Ziel: $E[X] = $ Konst.

Lemma: Seien $a_1, a_2, \dots, a_K \geq 0$, $\sum a_i = 1$, dann ist

$$\sum (a_i)^2 \geq \frac{1}{K}.$$

Beweis:

$$\sum \left(a_i - \frac{1}{K}\right)^2 = \sum \left(a_i^2 - \frac{2a_i}{K} + \frac{1}{K^2}\right)$$

$$= \sum a_i^2 - \frac{2}{K} \underbrace{\sum a_i}_{=1} + \sum \frac{1}{K^2}$$

$$= \sum a_i^2 - \frac{2}{K} + \frac{1}{K}$$

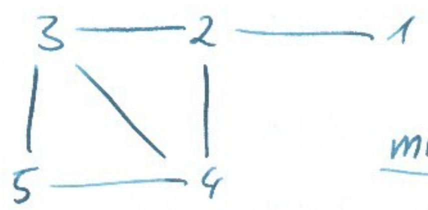
$$= \sum a_i^2 - \frac{1}{K} \geq 0$$

$$\Rightarrow \sum a_i^2 \geq \frac{1}{K}$$

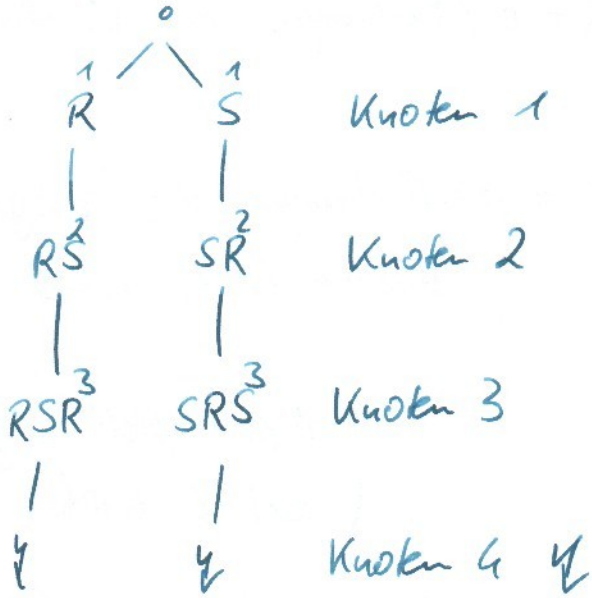
(Gleichheit bei $a_i = \frac{1}{K}$.

03.05.2018

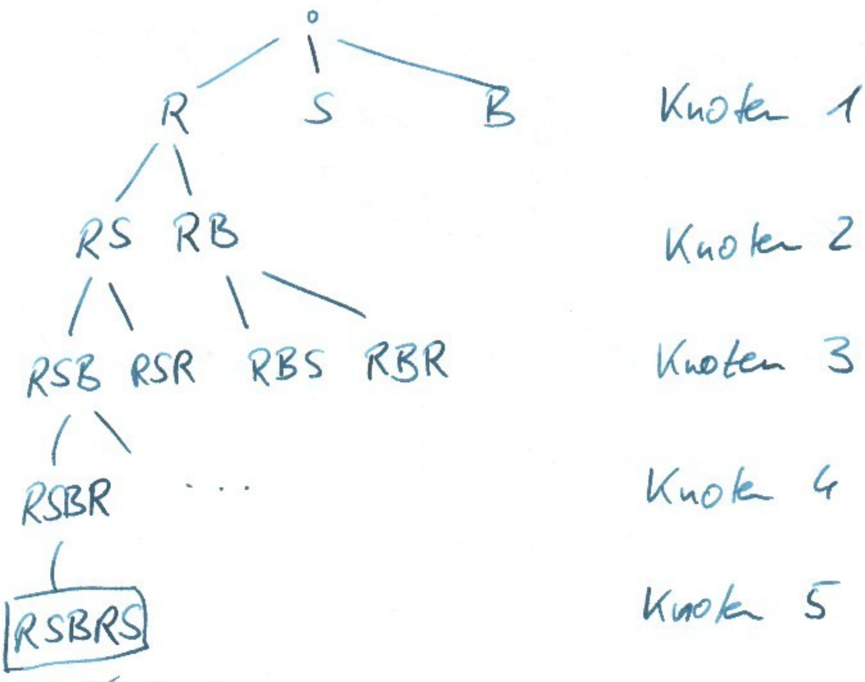
Graphfärbung, backtracking



mit 2 Farben



mit 3 Farben



Färbung gefunden!

3-Färbbarkeit.

Gegeben: Graph G

Frage: # Knoten des Backtrackingbaumes in Tiefe L = ...

Tiefe 1 = # 3Färbungen von Knoten 1

Tiefe 2 = # 3Färbungen von Knoten 1, 2

Tiefe 3 = # 3Färbungen von Knoten 1, 2, 3

⋮

Tiefe L = #3Färbungen des Teilgraphen auf Knoten $\{1, 2, \ldots, L\}$

(# prinzipiell möglicher 3-Färbungen auf L Knoten: 3^L)

Satz: Sei $C = (F_1, \ldots, F_L)$, $F_i \in \{R, S, B\}$ eine von den prinzipiell möglicher Färbungen.

#Graphen mit Knoten $\{1, \ldots, L\}$ und so daß C den Graphen richtig färbt ist

$$\leq 2^{L^2(1-\frac{1}{3})/2} = \sqrt[3]{2^{L^2}}$$

Beweis: C gegeben, $S_R = \#\{i \mid F_i = R\}$ $\quad S_R + S_B + S_S = L$

$$S_B = \#\{i \mid F_i = B\}$$

$$S_S = \#\{i \mid F_i = S\}$$

(16)

03.05.
2018

Welche Kanten sind erlaubt, so dass
C korrekt färbt?

$C = (.. R \dots S \dots)$ $\quad$ $\# \; S_R \cdot S_S + S_R \cdot S_B + S_S \cdot S_B$

$\underbrace{R \dots S}_{\text{erlaubte Kante}}$

$(S_R + S_S + S_B = L)$

$\left(\#\text{Graphen mit Färbung } C = 2^{S_R \cdot S_S + S_R S_B + S_S S_B} \right)$

Vermutung: Am Größten, wenn
$S_R \approx S_B \approx S_S = \frac{L}{3}$

$$S_R \cdot S_S + S_R S_B + S_S S_B = \frac{1}{2} \sum_{i \in \{R,S,B\}} \sum_{j \in \{R,S,B\}} S_i \cdot S_j - \frac{1}{2} \sum_{i \in \{R,S,B\}} S_i^2$$

$$= \frac{1}{2}(S_R + S_S + S_B)^2 - \frac{1}{2}(S_R^2 + S_S^2 + S_B^2)$$

$$\leq \frac{1}{2} L^2 - \frac{1}{2} \cdot \frac{L^2}{3}$$

$$= \frac{1}{2} L^2 \left(1 - \frac{1}{3}\right)$$

$\boxed{a_1, \dots, a_K, \; \sum a_i = 1 \quad \sum a_i^2 \geq \frac{1}{K}}$

hier: $S_1 + \dots + S_K = L$

$S_1^2 + \dots + S_K^2 \geq \frac{L^2}{K}$

$0 \leq \sum_{i=1}^{K} \left(S_i - \frac{L}{K}\right)^2$

$$\Rightarrow \#\text{Graphen} \leq 2^{L^2 \cdot \frac{1}{3}}$$

$\blacksquare$

Folgerung: $\#\{(C, G) \mid C$ färbt prinzipiell $\{1, \dots, L\}$,
G ist Graph auf $\{1, \dots, L\}$ der
richtig gefärbt wird$\}$

$$\leq 3^L \cdot 2^{\frac{1}{3}L^2}$$

Backtracking auf Zufallsgraph $\binom{n}{2}$, $\frac{1}{2}$.

$$\text{Prob}[G] = \left(\tfrac{1}{2}\right)^{\binom{n}{2}}$$

$X_L = \#$ Knoten des backtracking Algorithmus in Tiefe L.

$X = X_1 + X_2 + \dots + X_n$ $\quad E[X]$?

$$E[X_1] = 3$$

$$E[X_2] = \underbrace{\tfrac{1}{2} \cdot 9}_{\substack{\{1,2\} \\ \text{nicht} \\ \text{dabei}}} + \underbrace{\tfrac{1}{2} \cdot 6}_{\substack{\{1,2\} \\ \text{dabei}}} = \underline{\underline{\tfrac{1}{2} \cdot 15}}$$

Färbungen durchgehen, Graphen zählen, die die Färbung erlauben

$$= \underbrace{3 \cdot \tfrac{1}{2}}_{\substack{\text{Farbe gleich} \\ \to \text{Kante nicht da}}} + \underbrace{6}_{\substack{\text{Farbe} \neq \text{, Kante} \\ \text{egal.}}} = 7{,}5$$

$$E[X_L] \leq \underbrace{3^L \cdot 2^{\frac{1}{3}L^2}}_{\text{grob}} \cdot \left(\tfrac{1}{2}\right)^{\binom{L}{2}}$$

03.05.
2018

$$E[X] \leq \sum_{L=0}^{n} 3^L \cdot 2^{\frac{1}{3}L^2} \cdot \left(\frac{1}{2}\right)^{\binom{L}{2}}$$

$$= \sum_{L=0}^{n} 3^L \cdot 2^{\frac{1}{3}L^2} \cdot \frac{2^{\frac{L}{2}}}{2^{\frac{L^2}{2}}}$$

$$= \sum_{L=0}^{n} \left(3 \cdot 2^{\frac{1}{2}}\right)^L \cdot \frac{1}{2^{\frac{1}{6}L^2}}$$

$$= \sum_{L=0}^{n} \Bigg(\underbrace{\frac{3 \cdot 2^{\frac{1}{2}}}{2^{\frac{1}{6}L}}}_{<1}\Bigg)^L \leq \text{Konstante.}$$

für L groß genug, dann mit geom. Reihe.

$$\frac{1}{6}L > \log_2 \left(3 \cdot 2^{\frac{1}{2}}\right)$$

3. Chernoff-Schranken

(Verschärfungen des Gesetzes der Großen Zahlen.)

Beispiel:

Haben einen Graph mit $|E| = e$

Ziehen zufällige Menge $\text{Prob}[\text{Knoten}] = \frac{1}{2}$

Y ~~(e)~~ = #Kanten in der gezogenen Menge

$$Y = Y_1 + Y_2 + \ldots + Y_e$$

$$\text{Prob}[Y_i = 1] = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$$

$$E[Y] = \frac{1}{4} e$$

Zufallsgraph: S = feste Menge von der Hälfte der Knoten

$$Y = \#\text{Kanten in } S$$

$$Y = Y_1 + \ldots + Y_{\binom{n/2}{2}}$$

$$E[Y] = \frac{1}{2} \cdot \binom{\frac{n}{2}}{2} = \frac{1}{2} \frac{\frac{n}{2}\left(\frac{n}{2}-1\right)}{2} = \frac{1}{4} \cdot \frac{n^2}{4} \cdot (1 + o(1))$$

#Kanten $= \frac{1}{2}\binom{n}{2} = \frac{1}{4} n^2 (1 + o(1))$

03.05.2018

Satz: X binomialverteilt mit p, n.

$$\text{Prob}[X=k] = \binom{n}{k} p^k (1-p)^{n-k}$$

Es gilt: $\text{Prob}[X \geq (1+\delta)E[X]] \leq \Bigg(\underbrace{\frac{e^\delta}{(1+\delta)^{1+\delta}}}_{<1}\Bigg)^{E[X]}$

$$\text{Prob}[X \leq (1-\delta)E[X]] \leq \left(\frac{e^{-\delta}}{(1-\delta)^{1-\delta}}\right)^{E[X]}$$

Beweis: $t \gtrless 1$ wird später gewählt

$$\text{Prob}[X \geq (1+\delta)\cdot E[X]]$$

$$= \text{Prob}\left[t^X \geq t^{(1+\delta)E[X]}\right]$$

$$\leq \frac{E[t^X]}{t^{(1+\delta)E[X]}} \qquad \text{(Markov.)}$$

(X Zufallsvar.
neue ZV t^X
$(t^X)(\omega) := t^{X(\omega)}$)

$X = X_1 + X_2 + \ldots + X_n \quad X_i \in \{0,1\}$ alle unabhängig.

$$E[t^X] = E[t^{X_1+\ldots+X_n}] = E[\underbrace{t^{X_1}}_{1 \text{ oder } t} \cdot \ldots \cdot t^{X_n}]$$

(da X_i vollkommen unabhängig!) $= E[t^{X_1}] \cdot \ldots \cdot E[t^{X_n}]$

$$= \left(E[t^{X_1}]\right)^n$$

$$= (1(1-p) + t\cdot p)^n$$

$$= (1+(t-1)p)^n$$

$$\leq e^{(t-1)pn} = e^{(t-1)E[X]}$$

X, Y unabhängig
$\Leftrightarrow \text{Prob}[X=a \wedge Y=b]$
$= \text{Prob}[X=a] \cdot \text{Prob}[X=b]$

$$E[X\cdot Y] = \sum_{a,b} a\cdot b\cdot \text{Prob}[X=a \wedge Y=b]$$

$$= \sum_{a,b} a\cdot b\cdot \text{Prob}[X=a]\cdot\text{Prob}[Y=b]$$

$$= E[X]\cdot E[Y]$$

17.05.
2018

$$X_1 = \begin{cases} 1 & \text{mit Wkt. } p \\ 0 & \text{mit Wkt. } (1-p) \end{cases}$$

$$t^{X_1} = \begin{cases} t & \text{mit Wkt. } p \\ 1 & \text{mit Wkt. } (1-p) \end{cases}$$

$$E[t^{X_i}] = p \cdot t + (1-p) = 1 + p(t-1)$$

$$E[t^X] = (1 + p(t-1))^n$$

$$\leq e^{p(t-1)n} \qquad (1+x \leq e^x \text{ für } x \in \mathbb{R})$$

$$= e^{(t-1)E[X]}$$

Also aus der Markov-Ungl. gilt jetzt:

$$\text{Prob}[X \geq (1+\delta)E[X]] \leq \left(\frac{e^{t-1}}{t^{1+\delta}}\right)^{E[X]}$$

$$\leq \left(\frac{e^{\delta}}{(1+\delta)^{1+\delta}}\right)^{E[X]} \qquad (\text{mit } t = 1+\delta)$$

[andere Seite → Übung

$$\text{Prob}[X \leq (1-\delta)E[X]] \leq \left(\frac{e^{-\delta}}{(1-\delta)^{1-\delta}}\right)^{E[X]}$$

]

17.05.
2018

Folgerung:

$$\text{(a)} \quad \text{Prob}\left[X \geq (1+\delta)E[X]\right] \leq e^{-\frac{1}{3}\delta^2 \cdot E[X]}$$

$$\text{(b)} \quad \text{Prob}\left[X \leq (1-\delta)E[X]\right] \leq e^{-\frac{1}{2}\delta^2 \cdot E[X]}$$

Beweis: (a)

$$(1+\delta)^{1+\delta} = e^{(\ln(1+\delta))\cdot(1+\delta)}$$

Reihenentwicklung für $\ln$:

$$\ln(1+\delta) = \delta - \frac{\delta^2}{2} + \frac{\delta^3}{3} - \frac{\delta^4}{4} + \frac{\delta^5}{5} - \ldots$$

für $-1 \lneq \delta \leq 1$

$$(1+\delta)\cdot\ln(1+\delta) = (1+\delta)\left(\delta - \frac{\delta^2}{2} + \frac{\delta^3}{3} - \frac{\delta^4}{4} + \frac{\delta^5}{5} - \ldots\right)$$

$$= \delta - \frac{\delta^2}{2} + \frac{\delta^3}{3} - \frac{\delta^4}{4} + \frac{\delta^5}{5} - \ldots$$

$$+ \quad \delta^2 - \frac{\delta^3}{2} + \frac{\delta^4}{3} - \frac{\delta^5}{4} + \frac{\delta^6}{5} - \ldots$$

$$= \delta + \frac{1}{2}\delta^2 - \frac{1}{6}\delta^3 + \underbrace{\left(\frac{1}{3} - \frac{1}{4}\right)\delta^4}_{> 0}$$

$$+\left(\frac{1}{5} - \frac{1}{4}\right)\delta^5 \quad < 0$$

$$+\left(\frac{1}{5} - \frac{1}{6}\right)\delta^6 \quad > 0$$

$$+\left(\frac{1}{7} - \frac{1}{6}\right)\delta^7 \quad < 0$$

$$\ldots$$

$$\left(\frac{1}{i}-\frac{1}{i+1}\right)\delta^{i+1}+\left(\frac{1}{i+2}-\frac{1}{i+1}\right)\delta^{i+2}$$

$$\left(\frac{i+1-i}{i(i+1)}\right)\delta^{i+1}+\left(\frac{(i+1)-(i+2)}{(i+2)(i+1)}\right)\delta^{i+2}$$

$$\left(\frac{1}{i(i+1)}\right)\delta^{i+1}+\left(\frac{-1}{(i+2)(i+1)}\right)\delta^{i+2}\geq 0$$

$$(\text{da } 0\leq\delta\leq 1)$$

$$(1+\delta)^{1+\delta}\geq e^{\delta+\frac{1}{2}\delta^2-\frac{1}{6}\delta^3}$$

Damit ist

$$\frac{e^{\delta}}{(1+\delta)^{1+\delta}}\leq\frac{e^{\delta}}{e^{\delta+\frac{1}{2}\delta^2-\frac{1}{6}\delta^3}}=e^{-\frac{1}{2}\delta^2+\frac{1}{6}\delta^3}$$

$$\leq e^{-\frac{1}{2}\delta^2+\frac{1}{6}\delta^2}\quad(\text{da } \delta<1)$$

$$\leq \underline{\underline{e^{-\frac{1}{3}\delta^2}}}$$

(b) Zu zeigen: $\frac{e^{-\delta}}{(1-\delta)^{1-\delta}}\leq e^{-\frac{1}{2}\delta^2}$

$$(1-\delta)^{1-\delta}=e^{(\ln(1-\delta))(1-\delta)}$$

$$\cancel{-1\leq\delta\leq 1}$$

$$\cancel{\ln(1-\delta)=-\delta-\frac{\delta^2}{2}}$$

17.05.
2018

$$\ln(1+\delta) = \delta - \frac{\delta^2}{2} + \frac{\delta^3}{3} - \frac{\delta^4}{4} + \dots$$

$$\ln(1+(-\delta)) = -\delta - \frac{\delta^2}{2} - \frac{\delta^3}{3} - \frac{\delta^4}{4} - \dots$$

$$(1-\delta)\left(-\delta - \frac{\delta^2}{2} - \frac{\delta^3}{3} - \frac{\delta^4}{4} - \dots\right)$$

$$= -\delta - \frac{\delta^2}{2} - \frac{\delta^3}{3} - \frac{\delta^4}{4} - \dots$$

$$+ \delta^2 + \frac{\delta^3}{2} + \frac{\delta^4}{3} + \dots$$

$$= -\delta + \frac{\delta^2}{2} + \frac{1}{6}\delta^3 + \dots \geq -\delta + \frac{\delta^2}{2}$$

Damit: $\dfrac{e^{-\delta}}{(1-\delta)^{1-\delta}} \leq \dfrac{e^{-\delta}}{e^{-\delta + \frac{\delta^2}{2}}} = \underline{\underline{e^{-\frac{1}{2}\delta^2}}}$

$\delta \gg \frac{1}{\sqrt{n}}$, dann

$\delta^2 \cdot np \to \infty$

Anwendungsbeispiele (der Chernoff-Schranken)

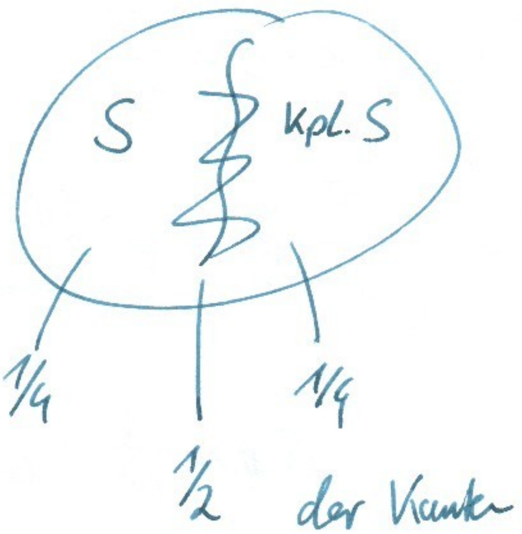
Zufallsgraph: $p = \frac{1}{2}$ $\quad S \subseteq \{1, \dots, n\}$ $\quad |S| = \frac{1}{2} n$

$$X = \#\text{Kanten in } S$$

$$E[X] = \binom{\frac{1}{2}n}{2} \cdot \frac{1}{2} = \frac{\frac{1}{2}n\left(\frac{1}{2}n - 1\right)}{2} \cdot \frac{1}{2}$$

$$= \frac{1}{4} \cdot \binom{n}{2} \cdot \frac{1}{2}$$

$$= \frac{1}{4} \cdot (\text{Gesamterwartungswert})$$



S fest!

Gilt das für alle(!) S mit $|S| = \frac{n}{2}$?

17.05.
2018

Mit Chernoff Schranken, festes S.

X ist verteilt mit $\binom{\frac{1}{2}n}{2}, \frac{1}{2}$.

$$\text{Prob}[X \geq (1+\delta)\, E[x]] \leq e^{-\frac{1}{3}\delta^2 E[x]} \overset{!}{\leq} 2^{-(n+f(n))}$$

$f(n) \to \infty$

<u>Dann:</u> $\text{Prob}[\text{Es gibt ein } S \text{ mit}$

$X \geq (1+\delta) E[x]] \leq 2^n \cdot \text{Prob}[X \geq (1+\delta) E[x]]$

$\to \underline{\underline{0}}$

$$E[x] \approx \frac{1}{4} n^2 \cdot \frac{1}{4}$$

$$-\frac{1}{3}\delta^2 E[x] = -\frac{1}{3}\delta^2 \cdot \frac{1}{16} n^2$$

$$2^n \cdot e^{-\frac{1}{3}\delta^2 \cdot \frac{1}{16} n^2}$$

$$= 2^{n - (\ln 2) \cdot \frac{1}{3}\delta^2 \cdot \frac{1}{16} n^2}$$

$$\leq \underline{\underline{2^{-\Omega(n^2)}}}$$

4. Hamilton-Kreis im Zufallsgraphen

Satz: Im Graphen mit $p = \frac{1}{2}$ finden wir mit Wkt. $\to 1$ in n einen Hamilton-Kreis.

Beweis: (in mehreren Schritten)

Für G gilt mit Wkt. $\to 1$:

① Für jeden Knoten v ist

$$\frac{n}{2} - \frac{n}{50} \leq |\mathcal{N}(v)| \leq \frac{n}{2} + \frac{n}{50}$$

$\mathcal{N}(v)$ = Nachbarn von v ohne v selbst.

Betrachte v fest Binomial mit $n-1, \frac{1}{2}$

$$E[x] = \frac{1}{2}(n-1)$$

$$\text{Prob}\left[|x - E[x]| \geq \frac{n}{50}\right]$$

$$\left(\frac{n}{50} = \frac{1}{25} E[x] (1+o(1))\right.$$

$$= \text{Prob}\left[|x - E[x]| \geq \frac{1}{25} E[x] (1+o(1))\right]$$

$$= \text{Prob}\left[(x - E[x])^2 \geq \left(\frac{1}{25}\right)^2 E[x]^2 (1+o(1))\right]$$

$$\leq \frac{E[x^2] - E[x]^2}{\left(\frac{1}{25}\right)^2 E[x]^2 (1+o(1))}$$

17.05.
2018

$$E[x^2] = E[x] + n(n-1)\cdot\frac{1}{4}$$
$$= E[x] + E[X]^2(1+o(1))$$

$$= \frac{E[x]}{(\frac{1}{25})^2\cdot E[x]^2} = \frac{1}{(\frac{1}{25})^2\cdot E[x]} = \underbrace{\frac{1}{(\frac{1}{25})^2\,\frac{1}{2}\cdot(n-1)}}$$

mal n für alle
Knoten gibt > 1
das nützt so nichts

↪ doch mit Chernoff ausrechnen.

24.05.
2018

Wiederholung Chernoff-Schranken:

X bin. Verteilt mit p, n $\quad E[X] = n \cdot p$

$$\text{Prob}[X \geq (1+\delta)\, E[X]] \leq e^{-\frac{1}{3}\delta^2 E[X]}$$

$$\text{Prob}[X \leq (1-\delta)\, E[X]] \leq e^{-\frac{1}{2}\delta^2 E[X]}$$

$$\text{Prob}[\, |X - E[X]| \geq \delta\, E[X]] \leq 2 e^{-\frac{1}{3}\delta^2 \cdot E[X]}$$

Weiter mit Hamiltonkreis:

Lemma 1: In G mit n Knoten, KantenWkt. $\frac{1}{2}$ gilt mit Wkeit $\to 1$:

Für jeden Knoten v ist

$$\frac{n}{2} - \frac{n}{50} \leq |N(v)| \leq \frac{n}{2} + \frac{n}{50} \qquad \left(E[N(v)] = \frac{1}{2}(n-1) \quad v \text{ fest} \right)$$

Beweis: Betrachte festes v, v beliebig.

$|N(v)|$ ist verteilt nach Binomialvert. mit $n-1$, $\frac{1}{2}$

$$\text{Prob}\left[|N(v)| \geq \frac{n}{2} + \frac{n}{50}\right] \leq e^{-\frac{1}{3}\delta^2 \cdot \frac{n}{2}} = e^{-c \cdot n}$$

c Kleine Konstante

$$\left(\left(\frac{n}{2} + \frac{n}{50}\right) = \underbrace{\frac{n}{2}}_{\approx E[|N(v)|]} \Big(1 + \underbrace{\frac{1}{25}}_{\delta}\Big) \right)$$

$$\text{Prob}\left[|N(v)| \leq \frac{n}{2} - \frac{n}{50}\right] \leq e^{-c \cdot n}$$

24.05.2018

$$\mathrm{Prob}\left[\left|\,|N(v)| - \frac{n}{2}\right| \geq \frac{n}{50}\right] \leq 2 \cdot e^{-c \cdot n} \leq e^{-c' n}$$

$$\mathrm{Prob}\Big[\,\left|N(1) - \frac{n}{2}\right| \geq \frac{n}{50} \text{ oder } \dots \text{ oder } \underbrace{\left|N(n) - \frac{n}{2}\right| \geq \frac{n}{50}}_{\leq e^{-c' n}}\Big]$$

$$\leq n \cdot e^{-c' n}$$

$$= e^{-c' n + \ln n} \to 0$$

(WKt, dass irgendein Knoten zu viel bzw zu wenige Nachbarn hat)

<u>Lemma 2</u> ~~tat~~ Mit WKt. $\to 1$ geltend:

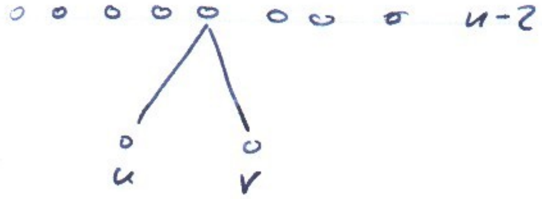
für alle u, v $u \neq v$ ist

$$\frac{3}{4}n - \frac{n}{50} \leq |N(u) \cup N(v)| \leq \frac{3}{4}n + \frac{n}{50}.$$

$$E[|N(u) \cup N(v)|] \geq \frac{n-1}{2}$$

$$|N(u) \cup N(v)| = |N(u)| + |N(v)| - |N(u) \cap N(v)|$$

$$E[|N(u) \cup N(v)|] = E[|N(u)|] + E[|N(v)|] - E[|N(u) \cap N(v)|]$$



$\cancel{E[\,|N(u)| \cap |N(v)|\,]}$

$$E[\,|N(u) \cap N(v)|\,] = \frac{1}{4}(n-2)$$

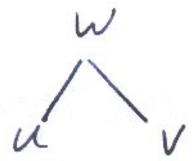
$$E[\,|N(u) \cup N(v)|\,] = \frac{3}{4}n(1 + o(1))$$

Beweis: $u \neq v$ fest, beliebig.

~~$|N(u) \cap N(v)|$ ist Verteilt nach bin. $n-2, \frac{1}{4}$~~

$$\cancel{E\left[|N(u) \cap N(v)|\right] = \frac{1}{4}(n-2) = \frac{1}{4}n\,(1+\underbrace{o(1)}_{-\frac{8}{n}})}$$

$|N(u) \cup N(v)|$ ist Verteilt bin. mit $n-2, \frac{3}{4}$.



$$\frac{1}{4} = \text{Prob}\left[w \notin (N(u) \cup N(v))\right]$$

$$\frac{n}{50} = \underbrace{\frac{4}{150}}_{\delta} \cdot \frac{3}{4}n$$

Chernoff:

$$\text{Prob}\left[\left|\,|N(u) \cup N(v)| - \frac{3}{4}n\right| \geq \frac{n}{50}\right]$$

$$\leq 2e^{-\frac{1}{3}\left(\frac{4}{150}\right)^2 \cdot \frac{3}{4}n}$$

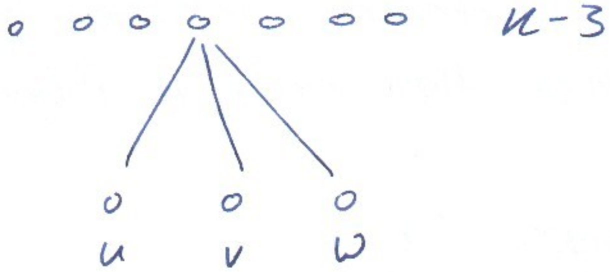
$$\leq e^{-c \cdot n}$$

$$\text{Prob}\left[\text{Es gibt } u,v \text{ mit } \left|\,|N(u) \cup N(v)| - \frac{3}{4}n\right| \geq \frac{n}{50}\right]$$

$$\leq n^2 \cdot e^{-c \cdot n} \leq e^{-cn + 2\ln n}$$

$$\to 0$$

24.05.2018



$|N(u) \cup N(v) \cup N(w)|$?

$\frac{1}{8}$ nicht dabei, $\frac{7}{8}$ dabei

<u>Lemma 2.3:</u> Mit Wkt $\to 1$ für alle u, v, w verschieden ist

$$\frac{7}{8}n - \frac{n}{50} \leq |N(u) \cup N(v) \cup N(w)| \leq \frac{7}{8}n + \frac{n}{50}.$$

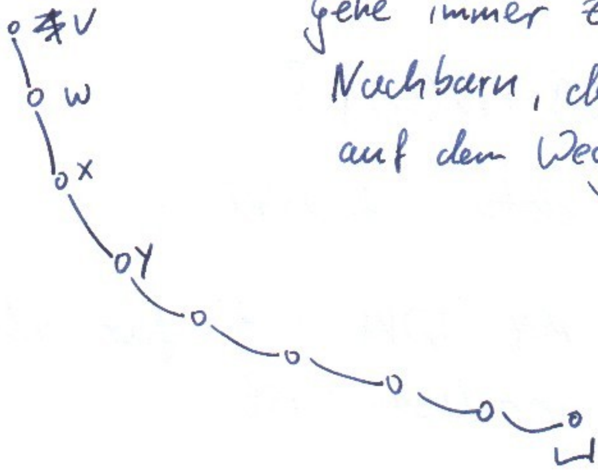
$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

$$\frac{3}{2} - 3 \cdot \frac{1}{4} + \frac{1}{8} = \underline{\underline{\frac{7}{8}}}$$

<u>Beweis:</u> analog zu 1 und 2.

Ziel: Für jeden Graph, der diese 3 Lemmas erfüllt, konstruieren wir einen Hamiltonkreis. Konstruktion (Algorithmus) in Polynomialzeit.

Phase 1: Langer Weg.

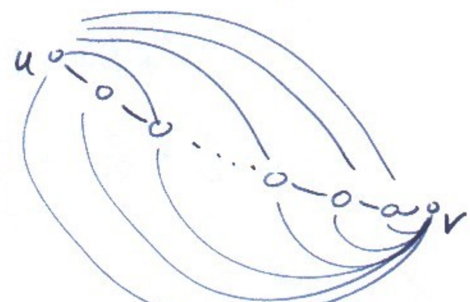


Gehe immer zu einem Nachbarn, der noch nicht auf dem Weg liegt.

$\geq \frac{n}{2} - \frac{n}{50}$ Nachbarn

Das garantiert einen Weg der Länge (= #Kanten = #Knoten − 1) mindestens $\frac{n}{2} - \frac{n}{50}$

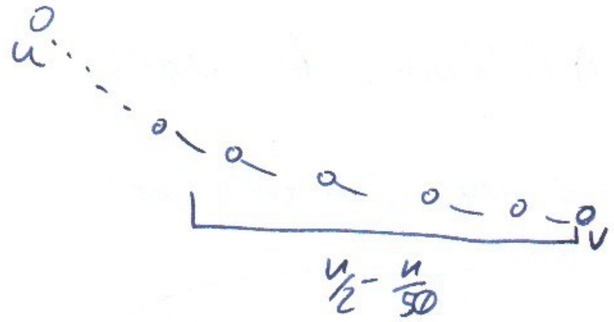
- Schlimmstenfalls, nur mit Lemma 1:



aber: nach Lemma 2: $|N(u) \cup N(v)| = \frac{n}{2} - \frac{n}{50}$ ausgeschlossen. !!!

24.05.
2018

~~[illegible]~~: Ist am Schwanz Schluß, dann am Kopf weiter!



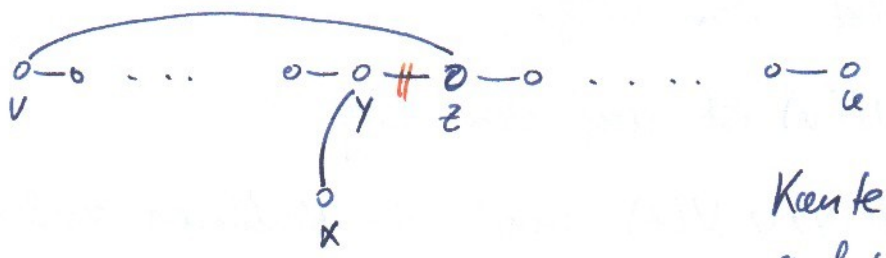
$$|N(u) \cup N(v)| \geq \frac{3}{4}n - \frac{n}{50}$$

Also Länge $\geq \frac{3}{4}n - \frac{n}{50}$.

Phase 2: Langer Weg: $\frac{7}{8}n - \frac{n}{50}$

~~#~~ Am Kopf und Schwanz ist Schluß.

Weg sieht folgendermaßen aus



Kante y-z auf Weg

x nicht auf Weg

Kante v-z im Weg

Sei es so!

y, z Streichen,

neuer Weg:

$x - y \rightsquigarrow v - z \rightsquigarrow u$

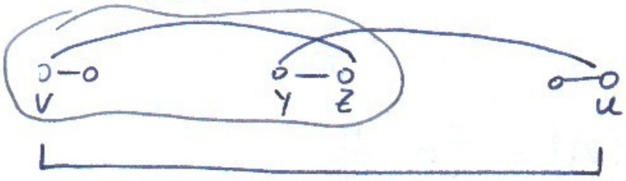
Wenn die Sit. ex. immer so weiter machen.

Warum ex. so ein x bzw. wann ex. <u>kein</u> x mehr?

Es ist nach Konstruktion

$N(u), N(v) \subseteq$ Kanten des Weges.

Es gibt $y-z$ auf dem Weg mit



$\leq \frac{7}{8}n - \frac{n}{50}$, von u aus $\frac{n}{2} - \frac{n}{50}$ Nachbarn.

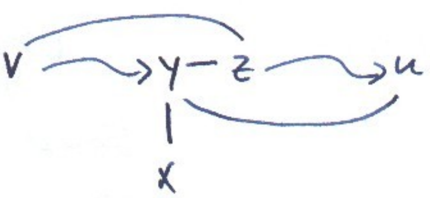
Würde das nicht auftreten, dann hätten wir für v nicht mehr genügend Nachbarn, da nur $\frac{3}{8}n$ übrig.

Nun ist $|N(u) \cup N(y) \cup N(z)| \geq \frac{7}{8}n - \frac{n}{50}$.

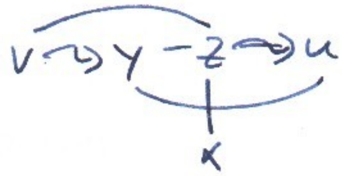
Nicht alle aus $N(u) \cup N(y) \cup N(z)$ sind auf dem Weg.

$N(v)$ ist auf dem Weg.

$N(y) \cup N(z)$ muß die Nachbarn außerhalb des Weges liefern. Also so:

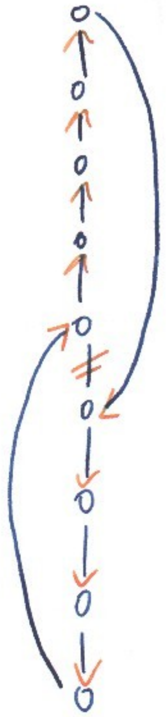


<u>oder</u>



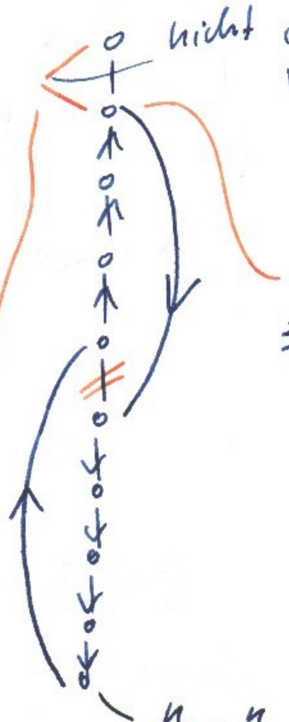
31.05.2018

Phase 3: Kreis bauen



gibt Kreis

oder



nicht auf Kreis

$\leq \frac{1}{8}n + \frac{n}{50}$ draußen

$\leq \frac{n}{2} + \frac{n}{50}$ auf dem Weg

Auf dem Weg

$> \frac{3}{4}n - \frac{n}{50} - \left(\frac{1}{8}n + \frac{n}{50}\right)$

$= \frac{5}{8}n - \frac{n}{25}$ $\cancel{\left(> \frac{n}{2}\right)}$

#1

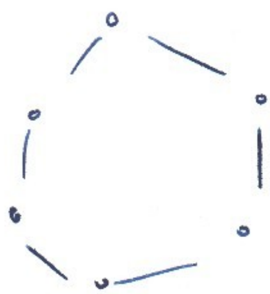
$\frac{5}{8}n - \frac{n}{25} > \frac{n}{2} + \frac{n}{50}$

$\frac{1}{8}n > \frac{3}{50}n$ ✓

$\Rightarrow$ Wir finden so eine Situation!

$\Rightarrow$ Kreis der Länge

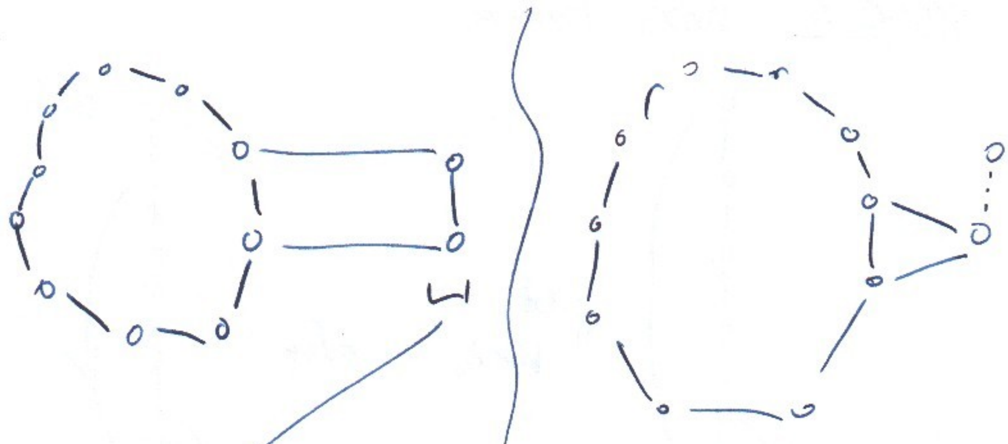
$\geq \frac{7}{8}n - \frac{n}{50} - 1$



$\leq \frac{1}{8}n + \frac{n}{50} + 1$ Knoten

TW

Knoten / Kanten in Kreis einbauen!



oder

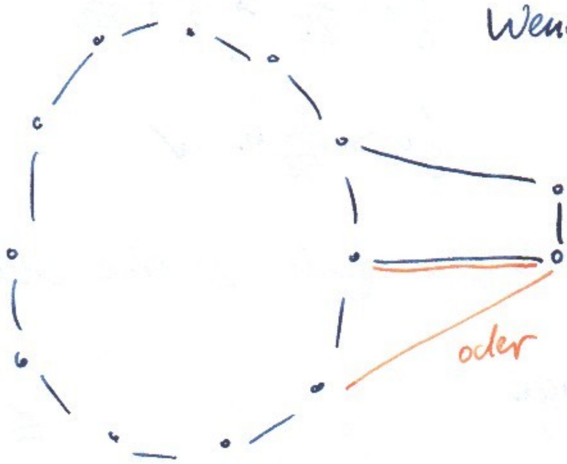
$\frac{3}{4}n - \frac{n}{50}$ Nachbarn

davon

$\geq \frac{3}{4}n - \frac{n}{50} - \left(\frac{1}{8}n + \frac{n}{50} + 1\right)$ im Kreis

$\frac{5}{8}n - \frac{n}{25} - 1$ im Kreis

$\geq \frac{n}{2}$



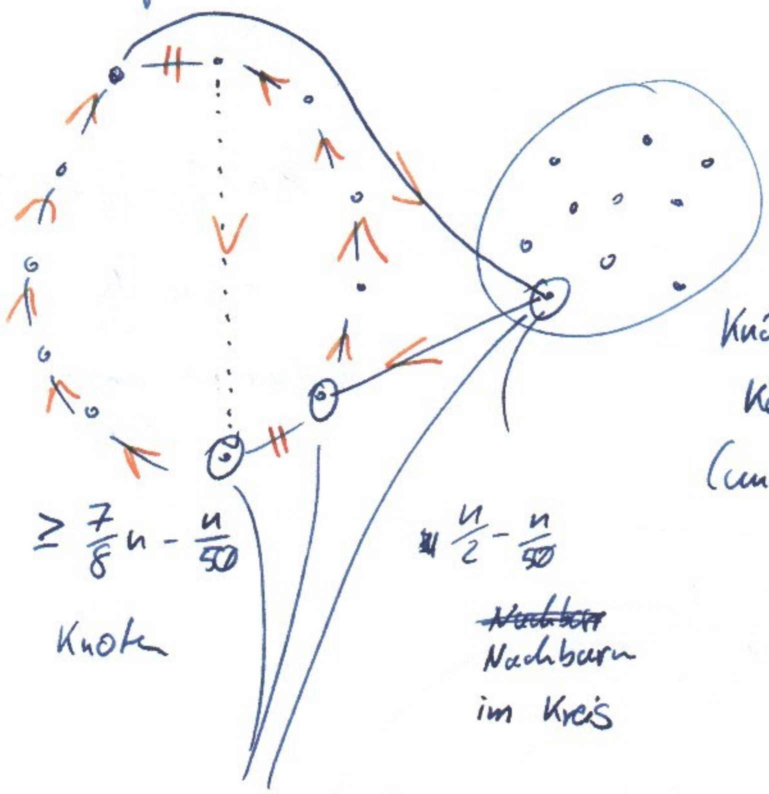
Wenn Nachbarn im Abstand 2 liegen reicht die Länge d. Kreises nicht!

Geht also immer.

31.05.
2018

Das geht solange, wie noch Kanten außerhalb vom Kreis liegen.

Situation jetzt:



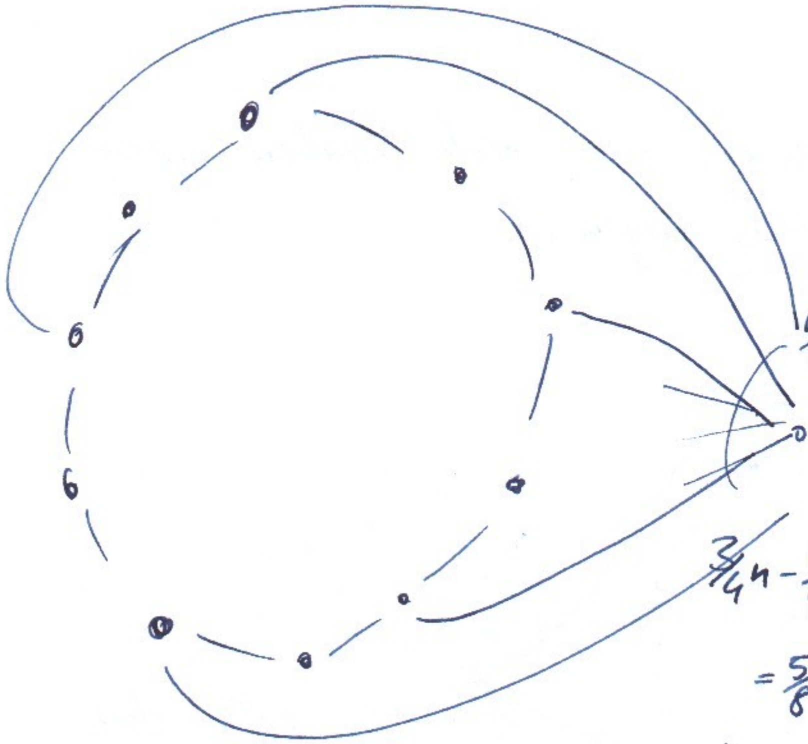
Knoten ohne Kanten (unabh. Menge.)

$\geq \frac{7}{8}n - \frac{n}{50}$ Knoten

$\geq \frac{n}{2} - \frac{n}{50}$ ~~Nachbarn~~ Nachbarn im Kreis

$\frac{3}{4}n - \frac{n}{50} - \left(\frac{1}{8} + \frac{n}{50}\right)$ im Kreis

$= \frac{5}{8}n - \frac{n}{25}$

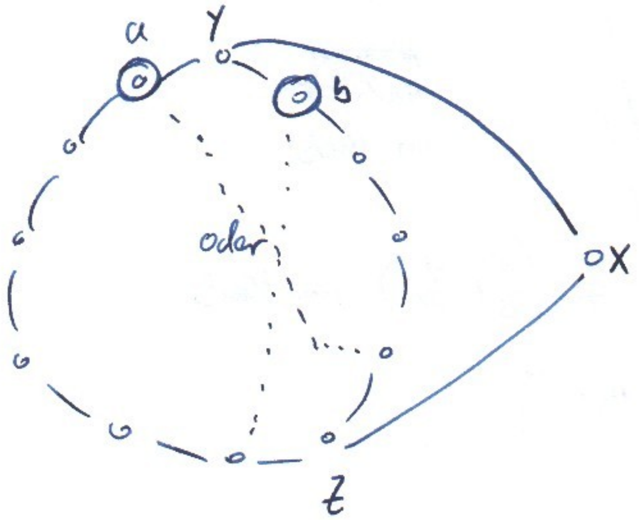


$\frac{n}{2} - \frac{n}{50}$

$\frac{3}{4}n - \frac{n}{50} - \left(\frac{1}{8}n + \frac{n}{50}\right)$

$= \frac{5}{8}n - \frac{n}{25}$

Nachbarn im ~~Kreit~~ Kreis



$\frac{n}{2} - \frac{n}{50}$ getroffen von X

$$\frac{3n}{4} - \frac{n}{50} - \left(\frac{1}{8}n + \frac{n}{50}\right) = \frac{5n}{8} - \frac{n}{25} > \frac{n}{2}$$

im Kreis von a, b aus

31.05.
2018

$\frac{n}{2} - \frac{n}{50}$ Knoten im Kreis

$\frac{n}{2} + \frac{n}{50}$ max. nicht getroffen der Kreis $< n$.

Mittlere ~~Lücke~~ Länge der Lücke

$\frac{n}{25}$ Jede 25'te Lücke > 1 ?

14.06.2018

Zum Local-Lemma:

$C \wedge F'$

$Prob_\alpha[C \wedge F'] \geq \left(1 - \frac{e}{2^k}\right) \cdot Prob_\alpha[F']$

$$Prob_\alpha[F'] = \underbrace{Prob_\alpha[C \wedge F']}_{\text{gesucht}} + \underbrace{Prob_\alpha[C \text{ falsch} \wedge F']}$$

$$\leq \dots \cdot Prob_\alpha[F']$$

$$\leq \frac{e}{2^k} \cdot Prob_\alpha[F']$$

$$Prob_\alpha[C \text{ falsch} \wedge F''] = \frac{1}{2^k} \cdot Prob_\alpha[F'']$$

$$Prob_\alpha[F'] \geq \frac{1}{e} \cdot Prob_\alpha[F'']$$

$$\Leftrightarrow Prob_\alpha[F''] \leq e \cdot Prob_\alpha[F']$$

$$Prob[C \text{ falsch} \wedge F'] \leq Prob[C \text{ falsch} \wedge F'']$$

$$= \frac{1}{2^k} \cdot Prob[F'']$$

$$\leq \frac{e}{2^k} \cdot Prob[F']$$

$$\Rightarrow Prob_\alpha[C \wedge F'] \cancel{=} \cancel{Prob_\alpha[C \text{ falsch} \wedge F'] - Prob_\alpha[F']}$$

$$= Prob[F'] - Prob[C \text{ falsch} \wedge F']$$

$$\geq Prob[F'] - \frac{e}{2^k} Prob[F']$$

$$= Prob[F'] \left(1 - \frac{e}{2^k}\right)$$

$$|\Gamma_F(C)| \leq \frac{2^k}{e} - 1$$

\# Vorkommen einer Variable x?

Bei maximalem Grad M ist

$$\# \Gamma_F(C) \leq k \cdot (M-1)$$

$$k \cdot (M-1) \leq \frac{2^k}{e} - 1$$

$$\Leftrightarrow \quad M - 1 \leq \frac{2^k}{k \cdot e} - \frac{1}{k}$$

Sicherlich wenn ~~#~~:

$$M \leq \frac{2^k}{e \cdot k}$$

$k = 10$

$\approx \frac{1000}{e \cdot 10}$

$M \leq \approx 30$

auf jeden Fall erfüllt die Bedingung!

14.06.2018

Frage: Kann ich eine erfüllende Belegung unter den Voraussetzungen des Local-Lemmas in Polynomialzeit finden?

Algorithmus: $\alpha : \{x_1, \dots, x_n\} \to \{0,1\}$

Eingabe: Formel F

1.) Wähle zufälliges α ($x_i = 0/1$ mit $\frac{1}{2}$)

1a) Teste, ob alle Klauseln wahr bei α.

2.) Nehme eine Klausel falsch unter α

C hat die Variablen $y_1, \dots, y_k$.

3) Ziehe für $y_1, \dots, y_k$ einfach zufällig neu, Rest bleibt.

$\rightsquigarrow$ neues α

Dann zu 1a).

Haben Tabelle von Zufallsbits, so organisiert:

	x_1	x_2	x_3	x_4 .	x_n	
1. Zug	1	0			1	für α am Anfang
2. Zug	0 C_1	1		. . 0	0	
3. Zug	1	0	C_2		1	
	↓	↓			↓	

• Lauf des Algorithmus $\hat{=}$ Folge von Klauseln von F

etwa $C_1, C_2, C_3, \dots, C_t$

1. neues ziehen 2. neues ziehen 3. neues ziehen ...

$C_1: x_1 \vee x_2$

$C_2: \neg x_2 \vee x_4$

Im Extremfall:

$C_1, C_1, C_1, C_1, \dots$

$\frac{1}{2^k}$ $\frac{1}{2^k}$ ...

C_i = das C aus dem Algorithmus im i'ten Lauf der Schleife.

Welcher Teil der vorherigen Rechnung ist „relevant" für C_2?

1) C_2 hat mit C_1 keine gemeinsamen Variablen, ~~mit C~~ dann irrelevant für C_2.

2) C_2 hat gem. Var. mit C_1, dann

C_2
/
C_1

(gehen Rechnung zurück)

14.06.2018

Wie kann das bei C_4 aussehen?

$$\begin{tikzcd}[column sep=small] C_4 & C_4 \arrow[d, dash] & C_4 \arrow[d, dash] \\ & C_1 & C_2 \arrow[d, dash] \\ & & C_1 \end{tikzcd}$$

C_2 ~ C_2 hat mit C_4 gem. Var.

C_1 ~ C_1 hat mit C_2 gem. Var.

C_3 hat keine gem. Var. mit ~~C_1, C_2~~ C_1 oder C_2

<u>allgemein</u>: Baum zu Klausel C_t (Rechnung $\overrightarrow{C_1, \dots, C_t}$)

1. Wurzel C_t

- Gehe zurück bis zur ersten Klausel, die zu C_t nicht disjunkt ist. Schreibe diese als Kind an C_t

$$\begin{tikzcd} C_t \arrow[d, dash] \\ C_s \end{tikzcd} \qquad s<t \qquad \overleftarrow{C_1, \dots, C_s, \dots, C_t}$$

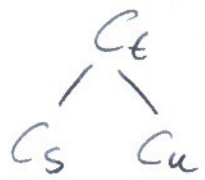
keine gem. V. mit C_t

- Gehe weiter zurück bis zur nächsten Klausel C_u, die mit C_t oder C_s gem. Var. hat. Hat C_u <u>nur</u> mit C_s was gemeinsames hat, dann Baum

$$\begin{tikzcd} C_t \arrow[d, dash] \\ C_s \arrow[d, dash] \\ C_u \end{tikzcd}$$

Auch wenn C_u mit C_s <u>und</u> C_t gem. V. hat.

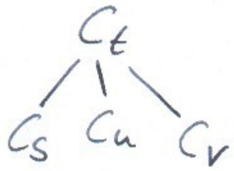
Hat aber C_u nur mit C_t gemeinsames, dann



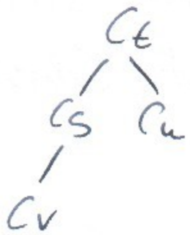
$u < s < t$

Weiter nach vorne: bis zur nächsten Klausel C_v, die mit dem Baum was gemeinsam hat.

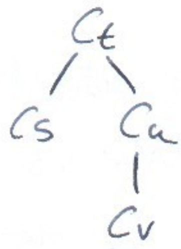
1. Fall C_v hat nur mit C_t:



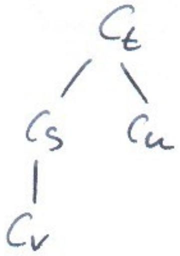
2. Fall C_v hat mit C_s, nicht C_u gemeinsam



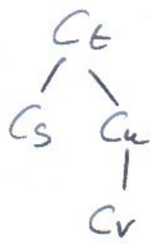
3. Fall nur mit C_u



4. Fall ~~nur~~ mit C_s, C_u dann



oder



14.06.2018

Allgemeiner Schritt:

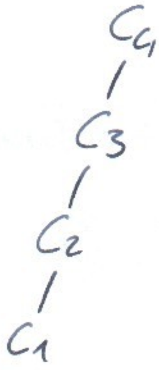
Haben Baum, Wurzel C_t
Kommen zu Klausel, die mit dem Baum was gemeinsam hat. (Klausel D).

Seien $D_1, \dots, D_l$ Klauseln im Baum, die mit D gemeinsam was haben.

$\Rightarrow$ hänge das D unter die im Baum tiefste Klausel im Baum von $D_1, \dots, D_l$

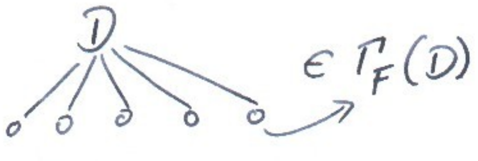
(falls mehrere tiefste, dann egal welches.)

Bsp.: C_1, C_2, C_3, C_4 $\quad C_i = C_i'$



Beobachtungen zu dem konstruierten Baum:

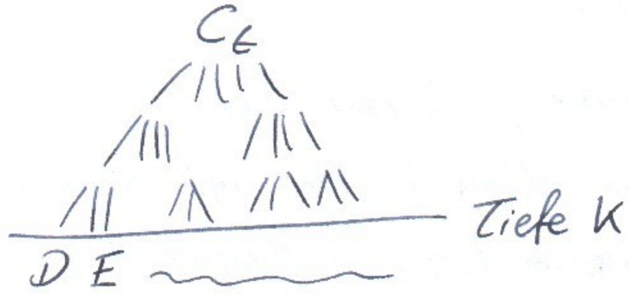
- max. Anzahl Kinder eines Knotens im Baum



Kinder von festem Knoten sind alle zueinander disjunkt

$\#\text{Kinder} \leq \#\Gamma_F(D)$

• Knoten auf einer Ebene



⇒ alle ~~Knoten auf~~ Klauseln in fester Tiefe sind alle disjunkt.

Haben Baum gegeben mit den vorher definierten Eigenschaften.

Was können wir über die zu Grunde liegende Rechnung ableiten?

Baum ist nur C_t

• WKeit eines solchen Baumes?

$$\le \frac{1}{2^k}$$

$\left(\frac{1}{2^k}\right)$ aus 1./2. Reihe

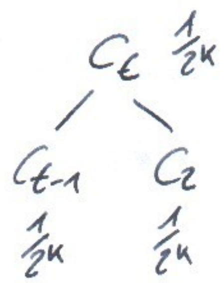
• WKeit des Baumes C_t — C_{t-1}

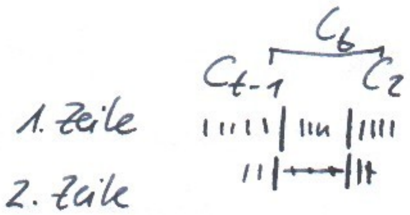
Rechnung: $C_1, \dots, C_{t-1}, C_t$

$\left(\frac{1}{2^k}\right)$ Zeile 1 der Tabelle

2. Reihe ⇝ Überschneidung mit C_t, die sind neu

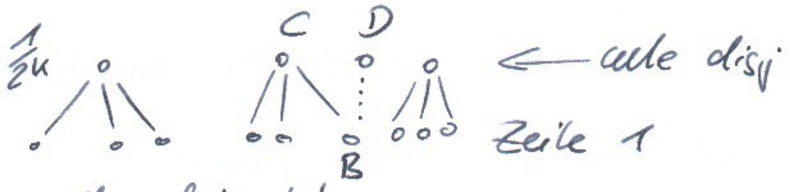
1. Reihe ⇝ noch nicht betrachten



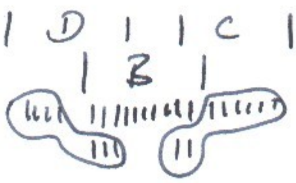


Baum mit ~~?~~ q Knoten (Klauseln)

$$\le \left(\frac{1}{2^k}\right)^{q}$$



alle disjunkt



$\Rightarrow$ Stufenweises hochgehen. An jeder Klausel, wenn sie falsch ist neue Zufallsbits.

D.h. Baum mit q Knoten hat W-keit $\le \left(\frac{1}{2^k}\right)^{q}$

Beobachtung: $q \geq 1$

$M = \#$ Klauseln in der Formel. Wenn der Algorithmus $q \cdot M$ Schritte läuft, dann hat er einen Baum ~~von~~

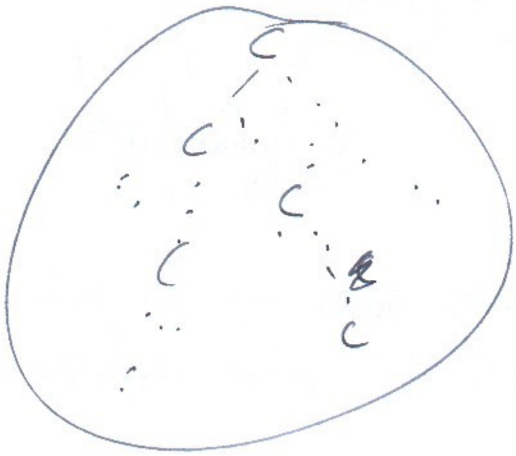
$$(C_1, C_2, \ldots, C_{q \cdot M})$$

mit $\geq q$ Klauseln.

$\Downarrow$

Wurzel: hinterste Klausel, die am häufigsten ist

Ist das C, dann Baum



21.06.
2018

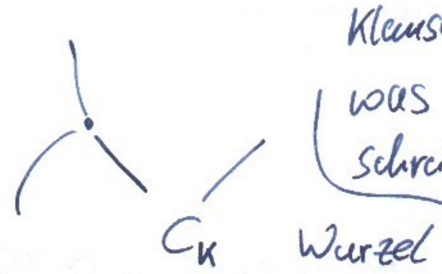
Rechnung des Algorithmus:

$C_1, C_2, \ldots, C_K, \ldots$

$\uparrow \quad \uparrow \qquad \uparrow$

falsch unter aktueller Belegung

Baum einer Klausel C_K auf der Rechnung.



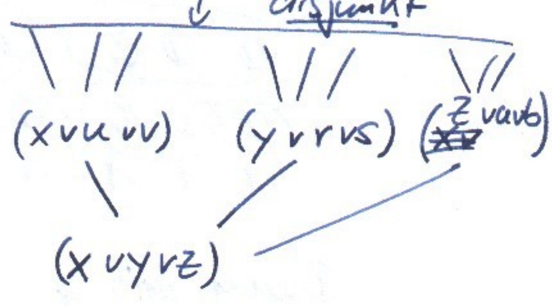
erste Klausel von hinten, die aus $\Gamma(C_K)$ ist (auch C_K selbst)

Findest Du die nächste Klausel, die mit dem Baum was gemeinsam hat, schreibe sie an die höchste Klausel, ~~die~~ mit der sie was gemeinsam hat. Falls mehrere höchste, dann freie Wahl.

$\Rightarrow$ In dem Baum ist <u>alles</u>, dessen Setzung Einfluß darauf hat, dass C_K vorkommt.

<u>Beispiele:</u> $C - C - C - C$ C immer falsch gezogen.

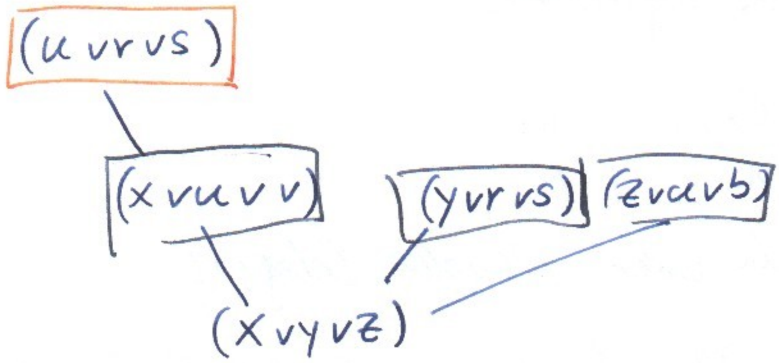
Klauseln auf einer ~~Ebene~~ Höhe sind alle disjunkt



#Kinder eines Knotens C

$\leq \# \Gamma(C)$ (Falls selbst Kind, dann nur 1 Kind!)

Haben Baum mit diesen Eigenschaften.



x	y	z	u	r	s	a	b	v
0	0	0	0	0	0	0	0	0
			0	0	0			

mögliche Rechnung:

$(u \vee r \vee s), \ldots, (x \vee u \vee v), \ldots, (y \vee r \vee s), \ldots, (z \vee a \vee b),$

$\ldots, (x \vee y \vee z)$

~~u~~	~~r~~	~~s~~	~~x~~	~~v~~	~~y~~	~~z~~	~~a~~	~~b~~
~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~
~~0~~	~~0~~	~~0~~	~~1~~	~~0~~	~~1~~	~~1~~	~~1~~	
	~~1~~	~~1~~						

u	r	s	x	v	y	z	a	b
0	0	0	0	0	0	0	0	0
0	0	0	0	1	0	0	1	1
1	1	1	1					

Baum mit q Klauseln tritt $\underbrace{\ }_{\text{in einer Rechnung}}$ auf: $\left(\frac{1}{2^k}\right)^q$

21.06.
2018

Wie hängen Rechnungslänge und möglicher Baum zusammen?

F hat M Klauseln.

Rechnung der Länge M^2:

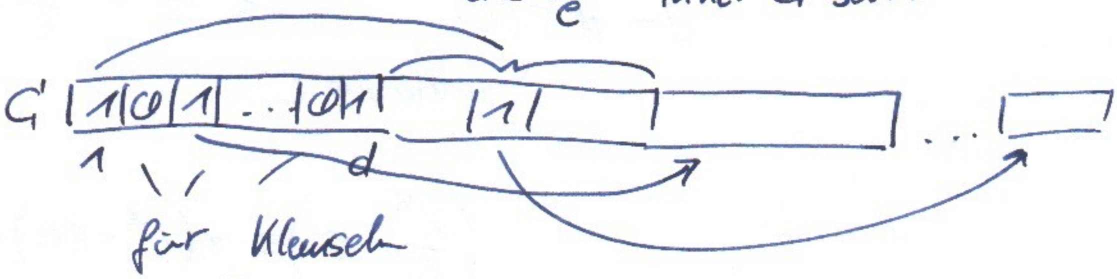
- Haben mind. eine Klausel, die $\geq M$ mal vorkommt.
- Baum des letzten Vorkommens dieser Klausel in der Rechnung hat $\geq M$ Knoten!

Wieviele Bäume mit q Klauseln haben wir?

Wurzel ist C (M Möglichkeiten)

Kennen wir $\Gamma(C) := (C_1, \dots, C_d)$

$d \leq \frac{2^k}{e}$ inkl. C selbst



$\#$ Einsen $= q-1$

$d \cdot q$ Bits

$\#$Bäume mit q Klauseln $\leq \underset{\substack{\uparrow \\ \text{Wurzel}}}{M} \cdot \binom{d \cdot q}{q-1}$ Viel mehr als die Anzahl der Bäume.

$$\leq M \cdot \binom{d \cdot q}{q} \leq M \cdot (d \cdot e)^q$$

$$\binom{d \cdot q}{q} = \frac{(d \cdot q)_q}{q!} \leq \frac{(d \cdot q)^q}{q!} \leq (d \cdot e)^q$$

$$\left(\begin{array}{l} e^q = 1 + q + \frac{q^2}{2} + \frac{q^3}{3!} + \ldots + \frac{q^q}{q!} + \ldots \\ e^q \geq \frac{q^q}{q!} \quad \Rightarrow q! \geq \frac{q^q}{e^q} \end{array} \right)$$

$$\leq M \cdot (2^k)^q \qquad \text{da } d \leq \frac{2^k}{e}$$

<u>Extra Voraussetzung:</u>

$$\underbrace{d = \# \Gamma(C)}_{\text{inklusive } C} \qquad < \frac{2^k}{e} = \frac{2^k}{e} - \varepsilon$$

$$\left(\frac{2^k}{e} - \varepsilon\right) e = (2^k - \varepsilon e) < 2^k$$

W-keit: Baum mit $\geq Q$ Knoten

$$\leq \sum_{q=Q} \left(\frac{1}{2^k}\right)^q \cdot (d \cdot e)^q \cdot M = \sum_{q=Q} \underbrace{\left(\frac{d \cdot e}{2^k}\right)}_{<1}^{q} \cdot M$$

$$= \underbrace{\left(\frac{1}{2^k} \cdot d \cdot e\right)^Q}_{\text{wird klein}} \cdot \overbrace{\frac{1}{1 - \frac{de}{2^k}}}^{\text{konst}} \cdot M$$

21.06.
2018

Wächst Q schneller als $\log_2 M$, dann geht das Ganze $\to 0$ in M.

Also W-Keit von Rechnungen $\geq M \cdot Q$ für Q schneller wachsend als $\log_2 M$ geht auch $\to 0$.

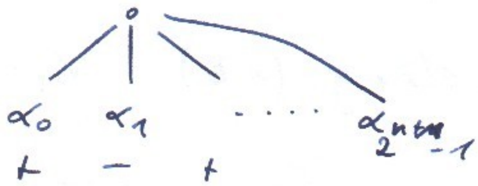
28.06.
2018

Randomisierte Algorithmen

Allgemeines aussagenlogisches Erfüllbarkeitsproblem. auf n Variablen

Eingabe: F

Erzeuge zufällige Belegung α.
Teste, ob F wahr bei α. Dann Ausgabe.



Ist F erfüllbar, dann

$$\text{Prob}[\text{Lösung gefunden}] \geq \frac{1}{2^n}$$

m unabhängige Läufe, W-keit m-mal keine Lösung gefunden

$$\leq \left(1 - \frac{1}{2^n}\right)^m$$

Ist etwa $m = 2^n \cdot n$, dann

$$\left(1 - \frac{1}{2^n}\right)^{2^n \cdot n} \leq e^{-1 \cdot n} = \left(\frac{1}{e}\right)^n \to 0$$

($\geq 2^n$ Läufe ist nicht gut, direktes Einsetzen ist besser!)

• Formeln in K-Konjunktiver Normalform.

Setzen die Variablen eine nach der anderen ein, vereinfache die Formel.

Vereinfache: $F = (\ldots) \wedge \ldots (x \vee \ldots) \wedge \ldots (\neg x \vee \ldots) \wedge \ldots$

$F_{|x=1} = (\ldots) \wedge \ldots$ Klausel streichen (wahr) $\wedge \ldots (\cancel{} \vee \ldots)$ x streichen (falsch)

$F_{|x=0}$ = analog

Setzung (z.B.) $x_1 = 1$, $x_3 = 0$, $x_5 = 1$

$F = \ldots \wedge (\neg x_1 \vee x_3 \vee \neg x_5 \vee x_{10}) \wedge \ldots$

$F_{|x_1=1, x_3=0, x_5=1} = \ldots \wedge (x_{10}) \wedge \ldots$

Jetzt muß $x_{10} = 1$ gesetzt werden!

Algorithmus: 1. Wähle zufällige Permutation der Variablen $x_1, \ldots, x_n$

~~$x_{i_1}, \ldots, x_{i_n}$~~ $\pi = \begin{pmatrix} 1 & \cdots & n \\ \pi(1) & \cdots & \pi(n) \end{pmatrix}$

$x_{\pi(1)}, \ldots, x_{\pi(n)}$

2. For $i = 1$ to n (Setzen von $x_{\pi(i)}$)

• falls in F eine Einerklausel $(x_{\pi(i)})$, dann auf 1; falls … $(\neg x_{\pi(i)})$, dann auf 0; sonst $x_{\pi(i)} = 0$ od. 1 mit Wkt. $\frac{1}{2}$

• $F = F$ vereinfacht gemäß $x_{\pi(i)}$

28.06.2018

3. Wenn alle Klauseln ~~...~~ weg sind, dann haben wir Lösung.

<u>Annahme</u>: F hat <u>genau eine</u> erfüllende Belegung.

<u>Also</u>: Ist α diese Belegung, dann gibt es für jedes x_i eine Klausel der Art

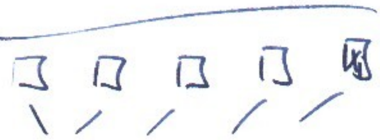
$$(\underbrace{x_l \vee \neg x_j \vee x_h}_{\text{Falsch unter } \alpha} \vee \underbrace{x_i}_{\alpha(x_i)=1}) \quad \text{oder} \quad (\underbrace{\dots}\vee \underbrace{\neg x_i}_{\alpha(x_i)=0})$$

Wahrscheinlichkeit, dass bei zufälligem π die Situation so ist, dass

$$x_l \; \dots \; x_j \; \dots \; x_h \; x_i$$

x_i als letztes gesetzt, alle anderen vorher $=0$

· im allgemeinen: $\frac{1}{K}$



$K!$ Mögl. Perm.

$(K-1)!$ „gute"

$\Rightarrow$ Wkt $\frac{1}{K}$

E[#Variablen, so dass sie als letzte der für sie zuständigen Klausel steht] $= n \cdot \frac{1}{k}$

Für so ein π ist $r(\pi)$ = #Variablen, die als letzte in der für sie zuständigen Klausel in π stehen.

$$E[r] = \frac{n}{k}$$

Was ist die Wahrscheinlichkeit, dass der Algorithmus α findet? (bei gegebenem π)

$$\geq \left(\frac{1}{2}\right)^{n-r(\pi)}$$

Prob[α wird gefunden und π ist gewählt]

$$= \frac{1}{n!} \cdot \left(\frac{1}{2}\right)^{n-r(\pi)}$$

$$\text{Prob}[\alpha \text{ gefunden}] = \sum_{\pi} \text{Prob}[\alpha \text{ gefunden und } \pi \text{ gewählt}]$$

$$\geq \sum_{\pi} \frac{1}{n!} \cdot \left(\frac{1}{2}\right)^{n-r(\pi)}$$

n! Summanden

$$= \left(\frac{1}{2}\right)^{n} \cdot \frac{1}{n!} \cdot \sum_{\pi} 2^{r(\pi)}$$

Jensen-ungl.

$$\geq \left(\frac{1}{2}\right)^{n} \cdot 2^{\frac{1}{n!} \sum_{\pi} r(\pi)} = \left(\frac{1}{2}\right)^{n} \cdot 2^{E[r]}$$

$$= \left(\frac{1}{2}\right)^{n} \cdot 2^{\frac{n}{k}}$$

28.06.
2018

$$\left(\frac{1}{2}\right)^n \cdot 2^{n/k} = \underline{\underline{\left(\frac{1}{2}\right)^{n(1-\frac{1}{k})}}}$$

Jensen Ungleichung:

X Zufallsvariable, $X \geq 0$, $f(x) \geq 0$
Konvex

$$E[f(X)] \geq f(E[X])$$

hier: $f(x) = 2^{-x}$

$X = r(\pi)$

2 einfache Fälle:

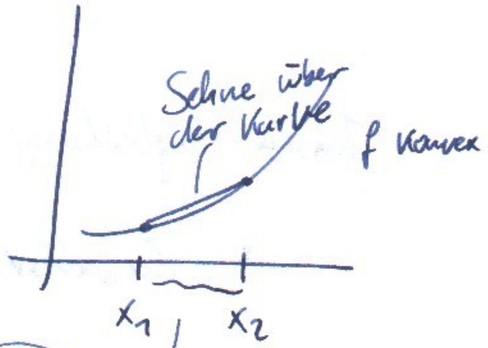
- $E[X^2] \geq (E[X])^2$ (aus $E[(X-E[X])^2] \geq 0$)
- $E[e^X] \geq e^{E[X]}$

denn
$$\begin{aligned}
E[e^X] &= E[e^{E[X]+X-E[X]}] \\
&= e^{E[X]} \cdot E[e^{X-E[X]}] \\
&\geq e^{E[X]} \cdot E[1+X-E[X]] \\
&= e^{E[X]} \cdot (E[1]+E[X]-E[X]) \\
&= e^{E[X]}
\end{aligned}$$

X hat endlich viele Werte.

~~Induktion über~~

Erst etwa 2 Werte.



Steigung:

$$\frac{f(x_2)-f(x_1)}{x_2-x_1}$$

Gerade: $f(x_1)+t\cdot\frac{f(x_2)-f(x_1)}{x_2-x_1}$

Punkte: $x_1+t(x_2-x_1)$

$0\leq t\leq 1$

$= x_1\cdot(1-t)+t\cdot x_2$

y-Wert der Geraden bei

$$x=(1-t)x_1+t\cdot x_2:$$

$$f(x_1)+t\cdot\bigl(f(x_2)-f(x_1)\bigr)=f(x_1)\,(1-t)+f(x_2)\cdot t$$

Konvexität:

$$f\bigl(x_1+t(x_2-x_1)\bigr)\leq f(x_1)+t\bigl(f(x_2)-f(x_1)\bigr)$$

$$\mathrm{Prob}[X_2] = t \quad , \quad \mathrm{Prob}[X_1] = 1-t$$

$$f(x_1 + t(x_2 - x_1)) = f(E[X]) \leq E[f(X)]$$

X hat Werte $x_1, \dots, x_n$

Wkeiten $\lambda_1, \dots, \lambda_n$; $\sum \lambda_i = 1$

Zeigen

$$\sum_{i=1}^{n} \lambda_i f(x_i) \geq f\left(\sum \lambda_i x_i\right)$$

$$\underbrace{\sum_{i=1}^{n} \lambda_i f(x_i)}_{E[f(X)]} = \cancel{\lambda_1} \; \lambda_1 f(x_1) + (1-\lambda_1) \cdot \underbrace{\sum_{i=2}^{n} \frac{\lambda_i}{1-\lambda_1} f(x_i)}_{\text{hier Ind.-vor. anwenden}}$$

$$\geq \lambda_1 f(x_1) + (1-\lambda_1) \cdot f\left(\sum \frac{\lambda_i}{1-\lambda_1} \cdot x_i\right)$$

$$\geq f\left(\lambda_1 x_1 + (1-\lambda_1) \sum \frac{\lambda_i}{1-\lambda_1} x_i\right)$$

$$= f\left(\sum \lambda_i x_i\right) = f(E[X])$$

S' = Menge der erfüllenden Belegungen

$\alpha \in S'$, $j(\alpha) = \#$ Variablen x_i mit

$$(\underbrace{x_l \vee x_k \vee x_m}_{\text{falsch}} \vee \underbrace{x_i}_{\text{wahr}}) \text{ oder}$$

$$(\ldots\ldots \vee \underbrace{\neg x_i}_{1 \text{ unter } \alpha.})$$

Für α; was ist der Erwartungswert bezüglich π der #Variablen von den $j(\alpha)$ vielen, die als letzte bzgl. der Klausel kommen:

$$\frac{j(\alpha)}{k}$$

$$\text{Prob}[\alpha \text{ wird erreicht}] \geq \cancel{\frac{1}{2^{n-j(\alpha)/k}}} \left(\frac{1}{2}\right)^{n-\frac{j(\alpha)}{k}}$$

bzgl. π und Zufallsbits

Ziel: $\frac{1}{2^{n(1-\frac{1}{k})}}$ da mehrere Belegungen zum Treffen sind.

05.07.
2018

3-SAT, n Variablen

1. zufällige Permutation von n: $\pi = \begin{pmatrix} 1 & \cdots & n \\ \pi(1) & \cdots & \pi(n) \end{pmatrix}$

2. setze die Variablen gemäß der Permutation

$$x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}$$

Setzen: $x_{\pi(i)}$

$i = 1, \ldots, n$

- 1 od. $\emptyset$ mit Wkt. $\frac{1}{2}$ wenn keine Klausel $(x_{\pi(i)})$ bzw. $(\neg x_{\pi(i)})$ existiert

  (kann auftreten, wenn

  $(x_{\pi(j)} \vee x_{\pi(i)} \vee x_{\pi(k)})$

  $j < k < i$ und

  $x_{\pi(j)} = x_{\pi(k)} = \emptyset$ gesetzt.)

- sonst $(x_{\pi(i)}) \rightsquigarrow = 1$

  $(\neg x_{\pi(i)}) \rightsquigarrow = \emptyset$.

(· Test auf alles erfüllt!)

1. $n!$

2. 1 od. 2 Mögl.

vereinfachende Annahme:

genau eine erfüllende Belegung.

$(b_1, \dots, b_n)$ erfüllende Belegung $b_i = 1$

$(b_1, \dots, \neg b_i, \dots, b_n)$ macht falsch.

Also muß eine Klausel der Art

$$\begin{array}{ccccc} (x_j & \vee & x_i & \vee & x_k) \\ \updownarrow & & & & \updownarrow \\ b_j & & & & b_k \\ & \searrow & & \swarrow & \\ & & \text{falsch} & & \end{array}$$

(für jedes x_i!)

Kritische Klausel für Bit i bezüglich x_i und der Belegung.

$\Rightarrow$ Haben also $\geq n$ Kritische Klauseln, ~~mit~~ für jede Variable mind. eine.

Beobachtung: Ist π so, dass

$$\cancel{\pi = \begin{pmatrix} \dots & k & \dots & i & \dots & j & \dots \\ & \pi(k) & & \pi(i) & & \pi(j) & \end{pmatrix}}$$

$$\pi = \begin{pmatrix} 1 & & & & n \\ \dots & j & \dots k \dots & i & \dots \end{pmatrix}$$

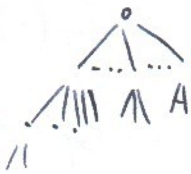
$$\Leftrightarrow \pi^{-1}(j) < \pi^{-1}(k) < \pi^{-1}(i)$$

mit W. $\frac{1}{2}$ auf b_j $\frac{1}{2}$ auf b_k

(mit Wkt. 1) wird richtig gesetzt!

$Prob_{\pi}[\, i$ steht hinter j und $k\,]$

1. Wähle Plätze für j, k, i



$\binom{n}{3}$

2. sortiere j, k, i an ihre Plätze

$\Rightarrow 6$ Mögl.

3. Rest verteilen

Wkt. f. 1 Blatt: $\dfrac{1}{\binom{n}{3} \cdot \cancel{6} \cdot (n-3)!}$

$$\binom{n}{3} \cdot \cancel{6} \cdot (n-3)!$$

$$\frac{n \cdot (n-1) \cdot (n-2)}{6} \cdot 6 \cdot (n-3)! = n!$$

$\Rightarrow$ Wkt. i als letztes: $\boxed{\frac{1}{3}}$ (allg. $\frac{1}{k}$)

Halte eine Permutation π fest. (bedingen darauf)

$r(\pi)$ = # Variablen, die bezogen auf π als letzte ihrer kritischen Klausel gezogen wird.

$$E_\pi[r] = \cancel{\#}\ n \cdot \frac{1}{3}$$

$$r = r_{\cancel{x_1}} + r_{\cancel{x_2}} + \ldots + r_{\cancel{x_n}}$$

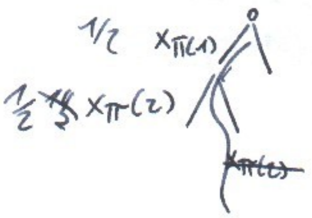
$$r_1 = \begin{cases} 1, & \text{gdw. } x_1 \text{ als letzte der Krit. Klausel von } x_1 \\ 0 & \text{sonst} \end{cases}$$

$$\text{Prob}[r_1 = 1] = \frac{1}{3}$$

Jetzt läuft der Setzprozess mit π. Erfolgswkt.?

Prob[Algo. trifft $(b_1, \ldots, b_n)$]

$$\begin{pmatrix} 1 & 2 \\ \pi(1) & \pi(2) \end{pmatrix}$$



genau ein Weg zu $(b_1, \ldots, b_n)$ $\rightsquigarrow$ $r(\pi)$ gibt es keine Wahl!

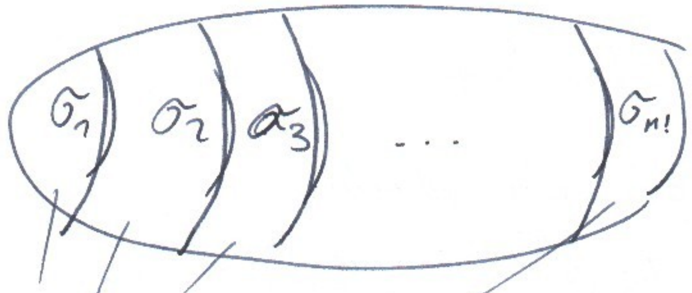
(ab $\pi(3)$ kann Wkt. = 1 sein)

$$\text{Prob}_\pi[(b_1, \ldots, b_n) \text{ getroffen}] = \left(\frac{1}{2}\right)^{n - r(\pi)}$$

Prob[Algo. trifft $(b_1, \ldots, b_n)$ wobei auch π gewählt wird]

$$= \sum_\sigma \text{Prob}[\pi = \sigma \wedge (b_1, \ldots, b_n) \text{ gesetzt}]$$

05.07.
2018



disj. Ereignisse.

$$= \sum_{\sigma} \left(\frac{1}{n!} \cdot 2^{-(n - r(\sigma))} \right)$$

$$= \left(\frac{1}{2}\right)^{n} \cdot \underbrace{\sum_{\sigma} \left(\frac{1}{n!} \cdot 2^{r(\sigma)} \right)}$$

r ist Zufalls var.

~~2^r ist~~ $2^r = f(r)$ ist auch ZV.

$$\sum_{\sigma} \frac{1}{n!} 2^{r(\sigma)} = E[2^r] = E[f(r)]$$

$$= \left(\frac{1}{2}\right)^{n} \cdot \underbrace{E[f(r)]}_{\substack{\geq \\ f(E[r])}}$$

$f = 2^r$ ist konvex

$$f(E[r]) = 2^{\frac{1}{n!} \sum_{\sigma} r(\sigma)}$$

$$\geq \left(\frac{1}{2}\right)^{n} \cdot 2^{E[r]} = \left(\frac{1}{2}\right)^{n} \cdot 2^{n/3}$$

$$= \underline{\underline{\left(\frac{1}{2}\right)^{(1-\frac{1}{3})n}}} = \left(\frac{1}{2}\right)^{2/3 n}$$

$m = 2^{\frac{2n}{3}} \cdot n$ Wiederholungen

Prob[$(b_1, \dots, b_n)$ nicht gefunden]

$$\leq \left(1 - \left(\tfrac{1}{2}\right)^{\frac{2n}{3}}\right)^{2^{\frac{2n}{3}}} \leq e^{-\left(\frac{1}{2}\right)^{2/3 n} \cdot 2^{2/3 n} \cdot n} = e^{-n}$$

$\rightarrow \underline{\underline{0}}$

<u>jetzt:</u> S = Menge aller erfüllenden Belegungen,

$|S| \geq 1$

Beliebige ~~erfüllung~~ erfüllende Belegung $(b_1, \dots, b_n)$ festgehalten.

$j(b)$ = # Kritische Variablen bzgl. $(b_1, \dots, b_n) = b$

$$\left(\begin{array}{ccccc} (x_j & \vee & x_i & \vee & x_k) \\ | & & \uparrow & & | \\ f. & & \text{krit.} & & f \end{array}\right)$$

π fest.; Prob[Algo findet $(b_1, \dots, b_n)$] $= \left(\frac{1}{2}\right)^{n - r(b,\pi)}$

$r(b, \pi)$ = # krit. Variablen bzgl. b, die ~~in~~ unter π ~~als~~ als letzte ihrer Klausel stehe

$(r(b,\pi) \leq j(b))$

05.07.2018

Prob[Algo mit Wahl von π findet $(b_1, \dots, b_n)$]

$$= \sum_{\sigma} \frac{1}{n!} \cdot \left(\frac{1}{2}\right)^{n - r(b,\sigma)}$$

$$\geq \left(\frac{1}{2}\right)^{n} \cdot 2^{E[r(b,\sigma)]}$$

$$= \left(\frac{1}{2}\right)^{n} \cdot 2^{\frac{j(b)}{3}}$$

Prob[Irgendeine erfüllende Belegung wird gefunden]

$$= \sum_{b \in S'} \underbrace{\text{Prob}[b \text{ wird gefunden}]}_{\geq \left(\frac{1}{2}\right)^{n - \frac{j(b)}{3}}}$$

$$\geq \sum_{b \in S'} \left(\frac{1}{2}\right)^{n - \frac{j(b)}{3}} = \sum_{b} \left(\frac{1}{2}\right)^{n + \frac{n}{3} - \frac{n}{3} - \frac{j(b)}{3}}$$

$$= \left(\frac{1}{2}\right)^{n\left(1 - \frac{1}{3}\right)} \cdot \underbrace{\sum_{b} \left(\frac{1}{2}\right)^{\frac{1}{3}\left(n - j(b)\right)}}_{\geq 1}$$

S irgendeine Menge von Belegungen $|S| \geq 1$

Für Belegung b ist $h(b) = \#$ Bits deren umsetzen ~~aus S rausführt~~. in S bleibt

$j(b) = \#$ Bits was rausführt

$h(b) = n - j(b)$

$$\sum_{b \in S} \left(\frac{1}{2}\right)^{n-j(b)}$$

$$= \sum_{b \in S} \left(\frac{1}{2}\right)^{h(b)} \overset{!}{\geq} 1$$

Ind. über n

$\underline{n=1}$ / $0/1$ $\frac{1}{2} + \frac{1}{2} = 1$ (IAnfang.)

1 $\frac{1}{2}^{h(b)} = 1$

$\underline{n \geq 1}$:

$S_0 = \{ c \in \{0,1\}^{n-1} \mid c0 \in S \}$

$S_1 = \{ c \in \{0,1\}^{n-1} \mid c1 \in S \}$

$S = S_0 \dot\cup S_1$

$\sum_{c \in S_0} \left(\frac{1}{2}\right)^{h(c)} \geq 1$ Ind vor.

ebenso $\sum_{c \in S_1} \left(\frac{1}{2}\right)^{h(c)} \geq 1$

05.07.
2018

1. Fall: $S_0 = \emptyset$ ($S_1 = \emptyset$ analog)

$$\sum_{b \in S} \left(\frac{1}{2}\right)^{h(b)} = \sum_{b \in S_1} \left(\frac{1}{2}\right)^{h_1(b)} \geq 1$$

2. Fall: $S_0 \neq \emptyset$, $S_1 \neq \emptyset$

$$\sum_{b \in S} \left(\frac{1}{2}\right)^{h(b)} = \sum_{c \in S_0} (1/2)^{h_S(c0)} + \sum_{c \in S_1} \left(\frac{1}{2}\right)^{h_S(c1)}$$

$$\geq \sum_{c \in S_0} \left(\frac{1}{2}\right)^{h_0(c)+1} + \sum_{c \in S_1} \left(\frac{1}{2}\right)^{h_1(c)+1}$$

≥ 1 mit Ind.-vor.

$\Rightarrow$ Laufzeit immer $2^{2/3 \cdot n}$

Algorithmus: Lokale Suche für K-KNF

Betrachten Formeln in 3-KNF, das ganze lässt sich aber auch auf K-KNF erweitern.

Also: F ist Formel in 3-KNF.

Die Idee ist die folgende:

- Wir starten bei einer beliebigen Belegung b und versuchen den Abstand zu einer (gedachten) erfüllenden Belegung a schrittweise zu verringern.
- Dazu kippen wir in jedem Schritt eine Variable in der Belegung b und fassen diese Variable danach nicht mehr an.
- Da wir nicht wissen, welche Variable „falsch" ist, also welche zu kippen ist, um näher an ~~die~~ eine Lösung zu kommen, müssen wir suchen!
- Die Suche ist nicht ganz blind, sondern orientiert sich an den ~~nicht~~ (noch) nicht erfüllten Klauseln in F.

- C_1 ist eine falsche Klausel von F.

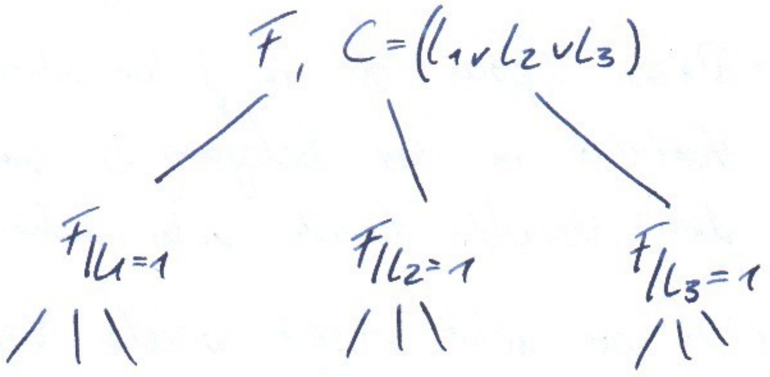
$$C = (l_1 \vee l_2 \vee l_3)$$

Literale

C ist falsch, d.h. die Variablen zu l_1, l_2, l_3 sind so gesetzt, dass diese ~~fals~~ alle falsch sind.

Falls F erfüllbar ist, muß also mind. eines der Literale gekippt werden. Dann betrachten wir $F_{|l=1}$. ~~für alle~~

Also sieht die Suche etwa so aus



In $F_{|l=1}$ kommt die Variable hinter l nicht mehr vor, kann also auch nicht mehr umgesetzt werden.

- Dass das ganze funktioniert, sollte klar sein. Genügend große Suchtiefe vorausgesetzt, sind irgendwann auf <u>einem</u> Weg alle Variablen umgesetzt und die Formel entweder erfüllt oder leer. D.h. falsch under der resultierenden Belegung.

- Falls die Formel erfüllbar ist, verringert einer der Zweige den Abstand zu einer erfüllenden Belegung.

- Mit Suchtiefe n können wir alle ~~Belegun~~ 2^n Belegungen erreichen und somit auch eine existierende erfüllende Belegung finden.

<u>Hammingabstand</u>: Haben wir 2 Belegungen a und b, dann bezeichnet der Hammingabstand $d(a,b)$ die #Stellen, an denen sich a und b unterscheiden.

- Starten wir bei b, dann hat jede erfüllende Belegung a ~~vo~~ von F den Hammingabstand

$$d(a,b) \leq n.$$

Die Suche hat dann eine Laufzeit von

$$\leq p(n) \cdot 3^n$$

für ein Polynom $p(n)$.

3 Aufrufe in jeden Rekursionsschritt, Tiefe $\leq n$

$p(n)$ brauchen wir für das Lesen der Formel, Finden einer falschen Klausel, Bilden von $F_{|L=1}, \ldots$

Das ist schlechter als einfach blind alle Belegungen zu testen!

Mit der folgenden Beobachtung lässt sich das aber deutlich verbessern!
Wir wählen geschickt mehrere Startpunkte und reduzieren die Suchtiefe.

2 Fälle: 1) Hat die erfüllende Belegung a mehr 0en als 1en, dann hat der Startpunkt $b_0 = 0^n$ einen Hammingabstand $d(a, b_0) \leq \frac{n}{2}$

2) Analog für $\#1 > \#0$ in a, dann $b_1 = 1^n$
$$d(a, b_1) \leq \frac{n}{2}$$

$\Rightarrow$ Wir machen die Suche 2x. Jeweils von b_0 und b_1 aus, mit ~~Tiefe~~ Suchtiefe $n/2$.

Die Laufzeit ist dann

$$\leq \cancel{p(n)}\, 2 \cdot \left(p(n) \cdot 3^{\frac{n}{2}}\right)$$

$$= \cancel{2 \cdot p(n) \cdot 2^{n \cdot \log}}$$

$$= 2 \cdot p(n) \cdot (1{,}732)^n$$

Also abgesehen von dem Polynom besser als 2^n. Das ist erstaunlich, geht das noch besser?

Mehr Startpunkte $\leadsto$ kleinere Suchtiefe

Trotzdem: Müssen alle 2^n mögl. Belegungen abdecken!

<u>Idee:</u> ◦ Suche im Hammingabstand r.

r hängt ab ~~vom~~ von der Variablenanzahl, also $r = \rho \cdot n$ mit $\rho \leq \frac{1}{2}$, kommt später.

◦ Wir nehmen eine zufällige Startbelegung. Wie ~~oft~~ oft müssen wir ansetzen, damit wir (mit hoher Wkt.) den gesamten Raum von 2^n Belegungen abdecken?

Damit eine feste Belegung a von der zufällig gezogenen Belegung b aus gefunden werden kann, muß a in der Hammingkugel von b mit Radius r liegen.

Hammingkugel: alle Belegungen, die ~~sich~~ Hammingabstand $\leq r$ vom Mittelpunkt haben.

$V(a,r)$ = # Belegungen in Hammingkugel von a mit Radius r.

Prob[feste Belegung a wird von b aus gefunden]

= Prob[a liegt in Hammingkugel von b mit Radius r]

= Prob[b wird aus Hammingkugel von a mit Radius r gezogen]

Prob[b wird aus Hammingkugel von a mit Radius r gezogen]

$$= \frac{V(a,r)}{2^n} = \frac{\text{„gute* Belegung"}}{\text{„alle Belegungen"}}$$

~~nun ist (siehe Nebenrechnung)~~

$\cancel{V(a,r) \geq}$

Das heißt eine feste Belegung a wird nicht erfasst. mit Wkt.

Prob[a wird von b aus <u>nicht</u> gefunden]

$$= 1 - \frac{V(a,r)}{2^n}$$

Wir ziehen $n \cdot \frac{2^n}{V(a,r)}$ Belegungen

Prob[a wird von keiner der $n \cdot \frac{2^n}{V(a,r)}$ unabhängig gezogenen Belegungen erfasst]

$$= \left(1 - \frac{V(a,r)}{2^n}\right)^{\frac{2^n}{V(a,r)} \cdot n}$$

$$\leq e^{-n} \qquad \text{mit } (1-x) \leq e^{-x}$$

das geht gegen 0.

Wir haben sogar:

Irgendeine der 2^n Belegungen wird nicht erfasst.

Prob[nicht alle 2^n Belegungen erfasst]

$$\leq \sum_a \text{Prob}[a \text{ wird nicht erfasst}]$$

$$\leq 2^n \cdot e^{-n} = e^{n \cdot (\ln 2 - 1)} \to 0$$

für n groß!

$(\ln 2 = 0{,}69 < 1)$

Wir müssen die Suche also

$n \cdot \frac{2^n}{V(a,r)}$ mal wiederholen, dann

haben wir mit hoher Wkt. alles abgesucht und finden mit hoher Wkt. eine erfüllende Belegung, sofern sie existiert.

Das gibt eine Laufzeit von

$$p(n) \cdot n \cdot \underbrace{\frac{2^n}{V(a,r)} \cdot 3^r}$$

Der exponentielle Anteil muß jetzt besser als 2^n werden! (Damit sich das lohnt)

Brauchen eine Untere Schranke für $V(a,r)$:

$$V(a, r = \rho n) = \sum_{i=0}^{r} \binom{n}{i}$$

<u>Es gilt:</u> $$\underbrace{\frac{1}{\sqrt{8n\rho(1-\rho)}} \cdot 2^{h(\rho)n}}_{\text{das müßte sich aus der Stirling-formel ergeben. ???}} \leq \underbrace{V(a,r) \leq 2^{h(\rho)n}}_{\text{das bekommt man leicht, siehe Nebenrechnung}}$$

Damit ist die Laufzeit bei $n \cdot \frac{2^n}{V(a,r)}$ Runden

$$\leq \underbrace{p(n) \cdot n}_{} \cdot \frac{2^n}{2^{h(\rho)n}} \cdot \underbrace{\sqrt{8n\rho(1-\rho)}}_{} \cdot 3^{\rho n}$$

Poly (n)

$$= q(n) \cdot 2^{(1-h(\rho))n} \cdot 3^{\rho n}$$ für ein Polynom $q(n)$

$h(\cancel{x}\rho)$ ist die Entropiefunktion

$$h(\rho) := -\rho \log_2 \rho - (1-\rho) \log_2 (1-\rho)$$

Hammingkugel (Größe, d.h. Volumen und Abschätzung)

zur Hammingkugel von a gehören alle Belegungen, die sich von a nur in r (Radius) Stellen unterscheiden. Schreibe r im Bezug zur Variablenzahl.

$$r = \rho n$$

$V(n, r = \rho n)$ ist das Volumen

$$V(n, r = \rho n) = \sum_{i=0}^{r} \binom{n}{i}$$

Wie viel ist das etwa?

Dazu eine nützliche Abschätzung. (Mit der binomischen Formel)

Es ist $1 = (\rho + (1-\rho))^n$

$$= \sum_{i=0}^{n} \binom{n}{i} \rho^i (1-\rho)^{n-i}$$

$$= (1-\rho)^n \sum_{i=0}^{n} \binom{n}{i} \left(\frac{\rho}{1-\rho}\right)^i$$

$$\geq (1-\rho)^n \sum_{i=0}^{r} \binom{n}{i} \left(\frac{\rho}{1-\rho}\right)^i$$

$$\geq (1-\rho)^n \sum_{i=0}^{r} \binom{n}{i} \left(\frac{\rho}{1-\rho}\right)^r$$

mit $\frac{\rho}{1-\rho} \leq 1$

$\Leftrightarrow \rho \leq 1-\rho$

$\Leftrightarrow \rho \leq \frac{1}{2}$

$$1 \geq (1-\rho)^n \cdot \sum_{i=0}^{r=\rho n} \binom{n}{i} \left(\frac{\rho}{1-\rho}\right)^{\rho n}$$

$$= \rho^{\rho n} \cdot (1-\rho)^{(1-\rho)n} \cdot \sum_{i=0}^{\rho n} \binom{n}{i}$$

Daraus folgt:

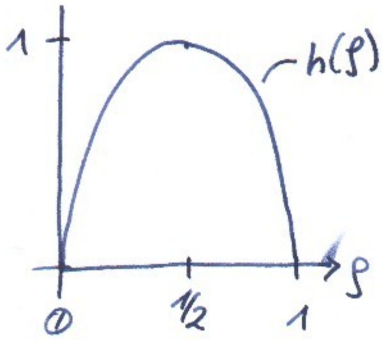
$$\Bigg(\underbrace{\left(\frac{1}{\rho}\right)^{\rho}}_{=2^{\rho\log\left(\frac{1}{\rho}\right)}} \cdot \underbrace{\left(\frac{1}{1-\rho}\right)^{1-\rho}}_{=2^{(1-\rho)\log\frac{1}{1-\rho}}}\Bigg)^n \geq \sum_{i=0}^{\rho n} \binom{n}{i}$$

Also:

$$2^{(-\rho\log\rho-(1-\rho)\log(1-\rho))n} \geq \sum_{i=0}^{\rho n} \binom{n}{i}$$

mit $h(\rho) = -\rho\log\rho - (1-\rho)\log(1-\rho)$ (Entropie-funktion)

$$\boxed{\sum_{i=0}^{\rho n} \binom{n}{i} \leq 2^{h(\rho)n}}$$



Die Abschätzung für $V(\alpha,r)$ nach der anderen Seite. Es ist tatsächlich so einfach, wie der Schöning das schreibt.

Es ist $\frac{1}{n+1} 2^{h(\rho)\cdot n} \leq V(\alpha,r) = \sum_{i=0}^{r} \binom{n}{i}$

$\left(\rho = \frac{r}{n} \ , \ r \leq n/2\right)$

Ansatz mit Binomialsatz:

$$1 = (\rho + (1-\rho))^n = \sum_{i=0}^{n} \binom{n}{i} \rho^i (1-\rho)^{n-i}$$

$$\leq (n+1) \cdot \max_i \left\{ \binom{n}{i} \rho^i (1-\rho)^{n-i} \right\}$$

Da $n+1$ Summanden. Das Maximum der Summanden liegt tatsächlich bei $i = \rho \cdot n$. Das sieht man, indem man sich die Differenz der Summanden i und $i+1$ für $0 \leq i \leq n-1$ ansieht.

<u>Also</u>:

$$1 \leq (n+1) \binom{n}{\rho n} \left(\rho^{\rho} (1-\rho)^{1-\rho}\right)^n$$

$\Leftrightarrow$

$$\frac{1}{n+1} \cdot \underbrace{\left(\left(\frac{1}{\rho}\right)^{\rho} \left(\frac{1}{1-\rho}\right)^{1-\rho}\right)^n}_{2^{n\cdot h(\rho)}} \leq \binom{n}{\rho n} \leq \sum_{i=0}^{\rho n} \binom{n}{i}$$

$$\binom{n}{i}\delta^{i}(1-\delta)^{n-i} \leq \binom{n}{i+1}\delta^{i+1}(1-\delta)^{n-i-1}$$

$$\Leftrightarrow \quad \binom{n}{i}\delta^{i}(1-\delta)^{n-i} \leq \binom{n}{i}\cdot\frac{n-i-1}{i+1}\cdot\delta\cdot\delta^{i}\cdot\frac{(1-\delta)^{n-i}}{(1-\delta)^{\cancel{n-i}}}$$

$$\Leftrightarrow \quad 1 \leq \frac{n-i-1}{i+1}\cdot\frac{\delta}{1-\delta}$$

$$\Leftrightarrow \quad (i+1)(1-\delta) \leq (n-i-1)\delta$$

$$\Leftrightarrow \quad 1-\cancel{\delta}+i-\cancel{i\delta} \leq n\delta-\cancel{i\delta}-\cancel{\delta}$$

$$\Leftrightarrow \quad 1+i \leq n\delta$$

$$\Leftrightarrow \quad i \leq n\delta-1$$

$\Leftrightarrow$ der Größte Wert liegt bei $\underline{\underline{i+1 \leq n\delta}}$

Jetzt müssen wir noch ein gutes ρ bestimmen.

Der exponentielle Anteil ist:

$$2^{\left(1-(-\rho\log\rho-(1-\rho)\log(1-\rho))+\rho\log 3\right)n}$$

im Exponent:

$$\left(1+\rho(\log\rho+\log 3)+(1-\rho)\log(1-\rho)\right)n$$

für $\rho=\frac{1}{4}$ wird das Minimal.

(Ableitung $\overset{!}{=}0$ setzen)

$$1+\frac{1}{4}\left(\log\frac{1}{4}+\log 3\right)+\frac{3}{4}\log\frac{3}{4}$$

$$=1-\frac{1}{2}+\frac{1}{4}\log 3+\frac{3}{4}\log 3-\underbrace{\frac{3}{4}\log 4}_{3/2}$$

$$=1-2+\log 3$$

$$=(\log 3)-1$$

<u>also</u>: $2^{(\log 3-1)n}=\frac{3^n}{2^n}=\underline{\underline{1{,}5^n}}$

allgemein erhält man $\rho=\frac{1}{k+1}$

und $\left(\frac{2k}{k+1}\right)^n\cdot p(n)$