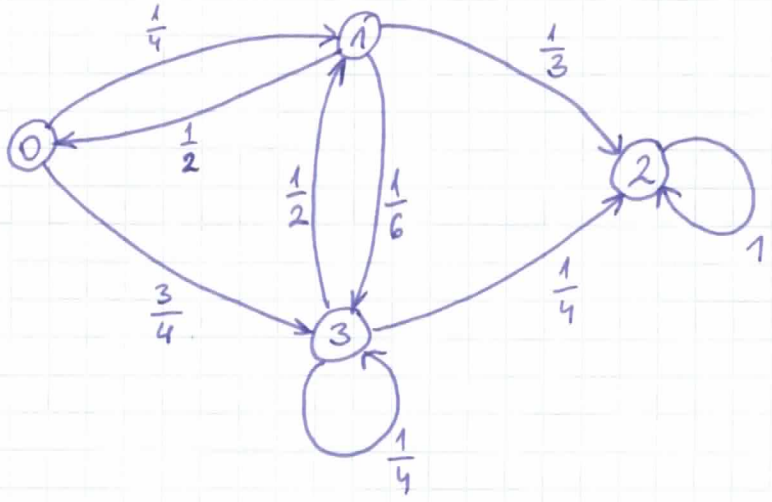
MARKOFF-KETTEN UND RANDOM WALKS

(Siehe auch Mitzenmacher-Upfal Kap. 7.)

Definition, Grundlagen

Beispiel: $\vec{G}(V, E)$ gerichteter Graph

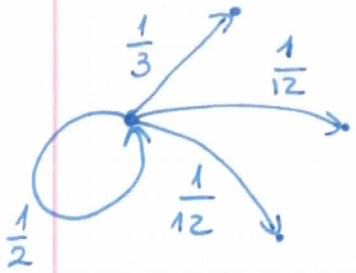


→ jede Kante (i,j) wird mit einem Wert $0 \leq p_{ij} \leq 1$ (Wahrscheinlichkeit) beschriftet

→ wir stellen uns vor, dass wir ein Random Walk auf dem Graphen durchführen, wobei wir in jedem Zeitschritt t von dem aktuellen Knoten über einer der ausgehenden Kanten zu einem Nachbarknoten gehen. Jede ausgehende Kante wird mit der Wahrscheinlichkeit gewählt, mit der sie beschriftet ist. $t = 0, 1, 2, \ldots$

Oder: die Knoten sind Zustände, und die Markoff-Kette wechselt ihren Zustand mit den gegebenen Wahrscheinlichkeiten. Die Beschriftungen der Kanten müssen also erfüllen:

Die Summe der Wahrscheinlichkeiten der ausgehenden Kanten eines jeden Knotens ist 1.



(Kanten mit $p_{ij} = 0$ werden nicht gezeigt)

Definition: Eine Markoff-Kette (G, P) besteht aus einem gerichteten Graphen $G = (V, E)$ und aus einer Übergangsmatrix $P = \{p_{ij}\}_{n \times n}$, wobei $n = |V|$, und p_{ij} die Wahrscheinlichkeit ist, dass in einem Schritt aus/von Zustand i, in den Zustand j gewechselt wird (die Knoten $v \in V$ werden auch Zustände der Markoff-Kette genannt).

Für die Matrix P gilt für jede Zeile i

$$\sum_{j=1}^{n} p_{ij} = 1$$

Eine solche Matrix nennt man stochastische Matrix.

Sei die Zufallsvariable X_t der Zustand der Markoff-Kette zum Zeitpunkt t. (für gegebene Anfangsposition/Anfangsverteilung)

Anwendungs-Beispiele (siehe Details später)

- die Knoten stehen für Lösungen in einem Lösungsraum, in dem ein Algorithmus mit Random Walk nach einer guten Lösung sucht.
- oder bestimmte Knoten werden in einem Graphen mit Random Walk gesucht

– oder eine Stichprobe von Punkten eines geometrischen Objekts wird mit Hilfe von Random Walks gesammelt.

Beispiel 1: Wir starten jeweils mit Wahrscheinlichkeit $\frac{1}{4}$ in dem Knoten 0, 1, 2 oder 3. Berechnen wir die Wahrscheinlichkeit, dass wir nach dem ersten Schritt im Knoten 3 sind

$$P(X_1 = 3) = \frac{1}{4} \cdot \frac{3}{4} + \frac{1}{4} \cdot \frac{1}{6} + \frac{1}{4} \cdot \frac{1}{4} + \frac{1}{4} \cdot 0$$

Im Allgemeinen, wenn q_i die Wahrscheinlichkeit ist, dass wir in i starten, dann für $V = \{1, 2, 3, \dots, n\}$

$$P(X_1 = j) = q_1 \cdot p_{1j} + q_2 \cdot p_{2j} + q_3 \cdot p_{3j} + \dots + q_n \cdot p_{nj}$$

(eigentlich ist diese die Formel für die totale Wahrscheinlichkeit mit den bedingten Wahrscheinlichkeiten

$$p_{ij} = P(X_t = j \mid X_{t-1} = i)$$

$$P(X_1 = 3) = P(X_0 = 0) \cdot P(X_1 = 3 \mid X_0 = 0) + P(X_0 = 1) \cdot P(X_1 = 3 \mid X_0 = 1) +$$
$$P(X_0 = 2) \cdot P(X_1 = 3 \mid X_0 = 2) + P(X_0 = 3) \cdot P(X_1 = 3 \mid X_0 = 3)$$

)

Beispiel 2. Wo wir starten ist irrelevant. Wie hoch ist die Wahrscheinlichkeit allgemein, dass die Kette von Zustand 1 in genau zwei Schritten in den Zustand 3 kommt? Bezeichne $p_{13}^{(2)} = P(X_t = 3 \mid X_{t-2} = 1)$

$$p_{13}^{(2)} = \underbrace{\frac{1}{2} \cdot \frac{3}{4}}_{\text{über } 0} + \underbrace{\frac{1}{6} \cdot \frac{1}{4}}_{\text{über Knoten } 3}$$

MK4.

Die allgemeine Formel für $V = \{1, 2, \ldots, n\}$ ist

$$p_{ij}^{(2)} = p_{i1} p_{1j} + p_{i2} \cdot p_{2j} + \ldots + p_{in} \cdot p_{nj} =$$

$$= \sum_{r=1}^{n} p_{ir} \cdot p_{rj}$$

Beispiel 3. Wie berechnet man die folgenden Wahrscheinlichkeiten?

a.) Wenn man mit Prob $= q_i$ in Knoten i startet, dann man in 2 Schritten in j ist?

b.) Dass man vom Zustand i in genau 3 Schritten in Zustand j kommt?

a.) $$P(X_2 = j) = q_1 \cdot p_{1j}^{(2)} + q_2 \cdot p_{2j}^{(2)} + \ldots + q_n \cdot p_{nj}^{(2)}$$

oder äquivalent

$$P(X_2 = j) = P(X_1 = 1) \cdot p_{1j} + P(X_1 = 2) \cdot p_{2j} + \ldots + P(X_1 = n) \, p_{nj}$$

b.) $$p_{ij}^{(3)} = \sum_{r=1}^{n} p_{ir}^{(2)} \cdot p_{rj} = \sum_{r=1}^{n} p_{ir} \cdot p_{rj}^{(2)}$$

Wir betrachten jetzt die Übergangsmatrix

$$P = \begin{bmatrix} p_{00} & p_{01} & p_{02} & p_{03} \\ p_{10} & p_{11} & p_{12} & p_{13} \\ p_{20} & p_{21} & p_{22} & p_{23} \\ p_{30} & p_{31} & p_{32} & p_{33} \end{bmatrix} = \begin{bmatrix} 0 & \frac{1}{4} & 0 & \frac{3}{4} \\ \frac{1}{2} & 0 & \frac{1}{3} & \frac{1}{6} \\ 0 & 0 & 1 & 0 \\ 0 & \frac{1}{2} & \frac{1}{4} & \frac{1}{4} \end{bmatrix}$$

→ Im Beispiel 1 haben wir den (Zeilen)-Vektor

$$q = \begin{bmatrix} \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \end{bmatrix}$$ mit dem letzten Spaltenvektor

$$\begin{pmatrix} p_{02} \\ p_{12} \\ p_{22} \\ p_{32} \end{pmatrix} = \begin{pmatrix} \frac{3}{4} \\ \frac{1}{6} \\ 0 \\ \frac{1}{4} \end{pmatrix}$$ multipliziert, und $P(X_1 = 3)$ erhalten.

Wenn wir mit Spalte p^j multiplizieren, ergibt das $P(X_1 = j)$

⟹ Allgemein:

Das Produkt $q \cdot P = [q_1\ q_2 \dots q_n] \cdot \begin{bmatrix} & & \\ & & \\ & & \\ & & \end{bmatrix} = [P(X_1=1), P(X_1=2) \dots]$

ergibt also die Wahrscheinlichkeitsverteilung von X_1 (Zustand nach dem ersten Schritt), falls die Anfangsverteilung $[q_1\ q_2 \dots q_n]$ war.

→ Im Beispiel 2. haben wir Zeile i von P mit Spalte j von P multipliziert, und $p_{ij}^{(2)}$ erhalten

$$\begin{bmatrix} \frac{1}{2} & 0 & \frac{1}{3} & \frac{1}{6} \end{bmatrix} \cdot \begin{bmatrix} \frac{3}{4} \\ \frac{1}{6} \\ 0 \\ \frac{1}{4} \end{bmatrix} = \begin{bmatrix} & & & p_{13}^{(2)} \end{bmatrix}$$

$P^{(2)}$

↓

Übergangsmatrix für 2 Schritte

Wir erhalten also alle Übergangswahrscheinlichkeiten $p_{ij}^{(2)}$ für genau 2 Schritte als die Einträge in der Produktmatrix

$$P \cdot P$$

→ laut 3.a.), wenn der Startzustand gemäß der Verteilung $q = [q_1\ q_2 \dots q_n]$ gewählt wird, dann ist die Verteilung von X_2 (Zustand nach dem 2-ten Schritt) $q \cdot P \cdot P$

$$\begin{bmatrix} & q & \end{bmatrix} \begin{bmatrix} & P & \end{bmatrix} \begin{bmatrix} & P & \end{bmatrix} = \begin{bmatrix} P(X_2=1), P(X_2=2) \dots & & P(X_2=n) \end{bmatrix}$$

→ laut 3.b.) ist die Übergangsmatrix für genau 3 Schritte $P^2 \cdot P = P^3$

Theorem: Sei $p_{ij}^{(k)}$ die Wahrscheinlichkeit, dass von Zustand i aus, nach k Schritten genau der Zustand j erreicht wird. Es gilt

$$p_{ij}^{(k)} = (P^k)_{ij}$$

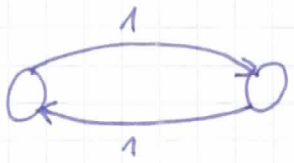
(der (i,j) Eintrag in der Matrix P^k) D.h. P^k ist die Übergangsmatrix für k Schritte.

Die Wahrscheinlichkeit, bei Startverteilung q, über einen zufälligen Weg von k Schritten den Knoten (genau) j zu erreichen $P(X_k = j)$ ist durch die j-te Komponente des Zeilenvektors $q \cdot P^k$ gegeben. D.h. $q \cdot P^k$ ist die Verteilung von X_k (bei Startverteilung q)

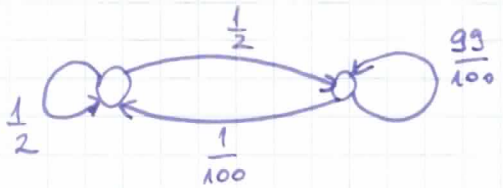
Beispiel: Betrachte das langfristige Verhalten einer Markoff-Kette. Was wird langfristig passieren

a.) im ersten Beispiel?

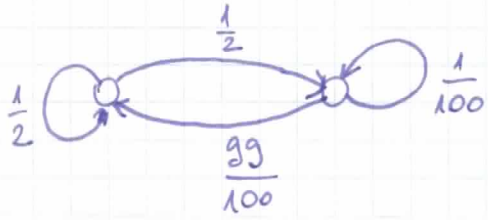
b.)



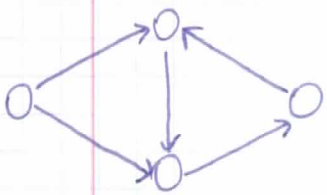
c.)



d.)



e.)



Beispiel: das 2-SAT Problem (siehe Mitzenmacher)

(2-SAT ist effizient lösbar. Hier betrachten wir das Verhalten einer zugehörigen Markoff-Kette, und bereiten uns auf 3-SAT vor.)

Eingabe: eine Formel in konjunktiver Normalform (CNF) wobei jede Klausel aus maximal 2 Literalen besteht

Ausgabe: entscheide ob es eine erfüllende Belegung gibt (falls ja, gib eine solche Belegung aus)

(Wiederholung der Begriffe:

Formel $\alpha = (x_1 \vee \bar{x}_2) \wedge (\quad) \wedge (\quad) \ldots$

n **Variablen** $x_1 \; x_2 \ldots x_n$

Literale $x_1 \; \bar{x}_1 \; x_2 \; \bar{x}_2 \; x_3 \; \bar{x}_3 \ldots x_n \; \bar{x}_n$

Klausel $(\bar{x}_1 \vee \bar{x}_3)$

α hat N Klausel: $\alpha = k_1 \wedge k_2 \wedge \ldots \wedge k_N$

im k-SAT Problem hat jede Klausel höchstens k Literale

Eine **Belegung** ist eine Zuweisung von 0-1 Werten zu den Variablen.

Die Anzahl der möglichen verschiedenen Belegungen ist 2^n.)

Beispiel: $(x_1 \vee \bar{x}_2) \wedge (x_2 \vee x_3) \wedge (\bar{x}_1 \vee \bar{x}_3)$ $n=3$, $N=3$

diese Formel ist erfüllbar

Ein randomisierter Algorithmus (lokale Suche, Random Walk)

1. wähle eine Belegung B zufällig (z.B. $(0, 1, 0)$)
2. wiederhole höchstens M- mal
   - 2a. akzeptiere B falls B die Formel erfüllt
     gib B aus, halt;
   - 2b. ansonsten gibt es mindestens eine Klausel k_e die nicht erfüllt wird (z.B. $(x_1 \vee \bar{x}_2)$ bei $(0,1,0)$)
     wähle zufällig eine Variable in k_e und flippe ihren Wahrheitswert (die unerfüllte Klausel k_e wird beliebig gewählt) (wähle x_1 oder x_2 zufällig, und setze $x_1 = 1$ bzw. $x_2 = 0$)
3. gib nicht-erfüllbar aus

Dieser ist ein Monte-Carlo Algorithmus mit einseitig beschränktem Fehler (Warum?)

(Wir könnten jetzt jede der 2^n möglichen Belegungen als die Zustände einer Markoff-Kette auffassen, und die lokale Suche (die Schritte des Algorithmus) als ein Random-Walk in dieser Markoff-Kette betrachten. (obwohl die Übergangswahrscheinlichkeiten schwer zu schätzen wären)
Wir definieren stattdessen eine einfachere Markoff-Kette mit Übergangswahrscheinlichkeiten, die (worst-case) Schätzungen

für die tatsächlichen Wahrscheinlichkeiten sind:)

Wir analysieren die Fehlerwahrscheinlichkeit in Abhängigkeit von der Anzahl der Wiederholungen M. Der Algorithmus irrt sich nicht, wenn es keine erfüllende Belegung gibt. Wir nehmen also an, dass die Eingabeformel erfüllbar ist, und fixieren eine beliebige erfüllende Belegung S. Wir schätzen die Wahrscheinlichkeit ab, während der lokalen Suche genau diese Lösung S zu treffen. (Sollten wir früher eine andere erfüllende Belegung S' finden, dann umso besser für die Laufzeit.) (bzw. für die Fehlerwahrscheinlichkeit)

→ Die Markoff-Kette habe die Zustände $\{0, 1, 2, \ldots, n\}$

Der Random-Walk sei im Zustand $X_t = j$ im Schritt t, wenn die aktuelle Belegung B genau j Variablen hat mit dem selben Wahrheitswert wie in S.

(Im Beispiel sei $S = (1, 1, 0)$ die fixierte erfüllende Belegung. Mit $B = (0, 1, 0)$ starten wir also im Zustand $X_0 = 2$. Unser Ziel ist es, mit dem Random Walk in den Zustand 3 zu kommen.)

Wie sieht die Markoff-Kette aus, und wie hoch sind die Übergangswahrscheinlichkeiten?

→ Vom Zustand j kommt der Algorithmus in den Zustand $j-1$ oder $j+1$, weil genau ein Wahrheitswert geflippt wird. Falls $X_t = n$, dann sind alle Wahrheitswerte genau wie in S, und B wird akzeptiert:

→ Von 0 kommen wir mit prob = 1 in Zustand 1

→ Sei z.B. $(x_1 \vee \bar{x}_2)$ die gewählte unerfüllte Klausel.

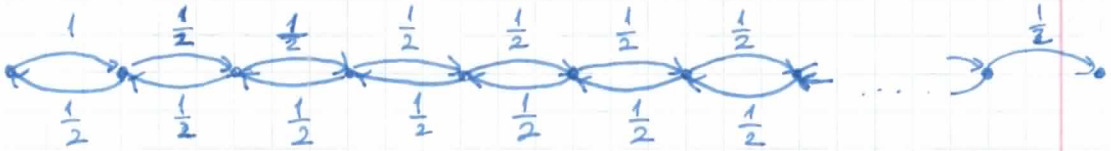
Dann gilt $x_1 = 0$ und $x_2 = 1$ in der aktuellen Lösung B, und in S gilt $x_1 = 1$ ODER $x_2 = 0$ ("ODER" beide).

Dementsprechend trifft der Algorithmus mit Wahrscheinlichkeit $\frac{1}{2}$ (ODER 1) eine Variable (x_1 o. x_2) deren Flippen die Lösung B zur S näher bringt von Zustand j nach j+1

$$P_{jj+1} \geq \frac{1}{2} \quad (\text{weil } \tfrac{1}{2} \text{ oder } 1)$$

$$P_{jj-1} \leq \frac{1}{2} \quad (\text{weil } \tfrac{1}{2} \text{ oder } 0)$$

Wir nehmen somit „worst-case" an, wenn wir jeder Kante die Übergangswahrscheinlichkeit $\frac{1}{2}$ geben.



Uns interessiert die erwartete Anzahl der Runden (Wert-Flippen) bis der Zustand n erreicht wird.
Dieser Erwartungswert hängt (sehr) davon ab, wo der Random Walk startet (also von der Anzahl der gemeinsamen Bits von dem ersten B mit S).

MK 12.

Def: Für die oben definierte Markoff-Kette, sei h_j die erwartete Anzahl der Schritte bis n erreicht wird, wenn der aktuelle Zustand j ist.
(bedingter Erwartungswert)

Offensichtlich ist h_0 (erwartete Schrittzahl von 0 gemeinsamen Werten) am höchsten, wir müssen also h_0 abschätzen.

→ es gilt

$$\boxed{h_n = 0}$$

wir brauchen nicht länger laufen, wir sind angekommen

→ versuchen wir h_0 mit Hilfe von h_1 auszudrücken:

$$\boxed{h_0 = 1 + h_1}$$

$$E[\text{nötige Schritte} \mid\mid \text{jetzt } 0] = E[\text{nötige Schritte} \mid\mid \text{jetzt } 1] + 1$$

→ h_{n-1} mit Hilfe von h_{n-2} und h_n

$$h_{n-1} = \frac{1}{2}\cdot 1 + \frac{1}{2}(h_{n-2}+1) = \frac{h_n}{2}^{0} + \frac{h_{n-2}}{2} + 1$$

Prob (wir laufen Richtung n)

nötige Schritte in diesem Fall

→ h_j mit Hilfe von h_{j-1} und h_{j+1}: $h_j = \frac{1}{2}(1+h_{j-1}) + \frac{1}{2}(1+h_{j+1})$

(*) $$\boxed{h_j = 1 + \frac{h_{j-1}}{2} + \frac{h_{j+1}}{2}}$$ für $j = 1, 2, 3, \ldots, n-1$

(Wir haben also $n+1$ Unbekannten $h_0\, h_1\, h_2 \ldots h_n$ und $n+1$ Gleichungen ⟹ es gibt eine eindeutige Lösung

Wir zeigen hier eine rekursive Lösung :)

Behauptung: $h_j = h_{j+1} + 2j + 1$

Beweis durch Induktion:

Basisschritt: $h_0 = h_1 + 2 \cdot 0 + 1 = h_1 + 1$

Induktionsschritt: $j-1 \to j$

$$h_{j+1} \overset{(*)}{=} 2h_j - h_{j-1} - 2 = 2h_j - (h_j + 2(j-1) + 1) - 2 =$$

$$= h_j - 2j - 1 \qquad \square$$

Mit Hilfe der Behauptung, können wir jetzt h_0 berechnen (streng genommen: auch mit Induktion):

$$h_0 = h_1 + 1 = (h_2 + 3) + 1 = h_3 + 5 + 3 + 1 =$$

$$= h_4 + 7 + 5 + 3 + 1 = \ldots\ldots\ldots = h_n + (2n-1) + (2n-3) + \ldots + 3 + 1 =$$

$$= 0 + \underbrace{n \cdot \frac{a_1 + a_n}{2}}_{\text{arithmetische Summe}} = n \cdot \frac{2n-1+1}{2} = n^2$$

es folgt:

Theorem: Für eine beliebige (sogar die schlimmste) Anfangsbelegung B, die <u>erwartete Anzahl</u> der Schritte bis die Belegung S (oder eine andere erfüllende Belegung) gefunden wird, ist höchstens n^2.

Wie lange sollte der Random Walk laufen bis die Suche aufgegeben wird?

Wir schätzen die Wahrscheinlichkeit nach oben ab, dass z.B. ein $2n^2$ langer Random Walk S nicht findet:

MK 14.

Bezeichne Z die Anzahl der Schritte, bis eine erfüllende Belegung gefunden wird.

Z ist eine Zufallsvariable, die von der Folge der Zufallsschritten (Münzwurfen) des Random Walks abhängt. Wir haben oben $E[Z] \leq n^2$ gezeigt.

→ Da $Z \geq 0$, die Markoff-Ungleichung ergibt

$$\text{Prob}\left(Z \geq 2n^2\right) \leq \frac{E[Z]}{2n^2} \leq \frac{n^2}{2n^2} = \frac{1}{2}$$

→ Wenn wir die Anzahl der Schritte auf $M = m \cdot 2n^2$ setzen, dann die Wahrscheinlichkeit, dass die fixierte Lösung S nicht getroffen wird, ist höchstens

$$\underbrace{\frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \ldots \cdot \frac{1}{2}}_{m \text{ mal}} = \frac{1}{2}^m$$

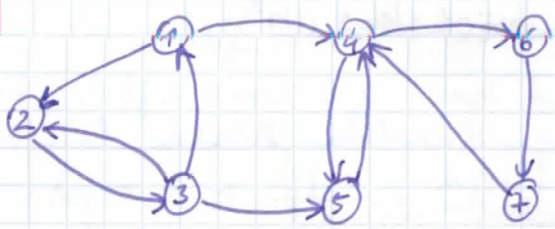
⇒ mit $M = m \cdot 2n^2$, die Fehlerwahrscheinlichkeit des Monte-Carlo Algorithmus ist höchstens $\frac{1}{2^m}$

Eigenschaften von Markoff-Ketten

(wir möchten das langfristige Verhalten von Markoff-Ketten vorhersagen)

1.) Irreduzible Markoff-Ketten

Beispiel:



jede Kante = positive Übergangswahrscheinlichkeit

Was könnte man über das langfristige Verhalten dieser Markoff-Kette vorhersagen?

→ irgendwann gerät die Markoff-Kette in einen der Zustände $\{4,5,6,7\}$, und kann zu den Zuständen $\{1,2,3\}$ nie wieder zurückkommen.

Definition: Sei $(\vec{G}(V,E), P)$ eine Markoff-Kette (so dass $p_{uv} > 0 \Leftrightarrow (u,v) \in E$). Ein Zustand j ist von einem anderen Zustand i <u>erreichbar</u>, wenn für mindestens ein $k \in \mathbb{N}$ die Wahrscheinlichkeit $p_{ij}^{(k)} > 0$

Behauptung: $j \in V$ ist erreichbar von $i \in V$

$\Updownarrow$

es gibt einen gerichteten Weg in G von i nach j

Bsp: ⑦ ist aus ② erreichbar, aber ② ist aus ⑦ nicht erreichbar

Definition: Die Markoff-Kette heißt <u>irreduzibel</u> wenn jeder Knoten j von jedem Knoten i erreichbar ist.

Beobachtung: (G,P) ist genau dann irreduzibel wenn von jedem Knoten i zu jedem Knoten j ein gerichteter Weg existiert, d.h. der Graph G <u>stark zusammenhängend</u> ist.

→ Wenn (G,P) reduzibel ist, dann gibt es also Knoten i,j so dass der Eintrag $p_{ij}^{(k)}$ in jeder der Matrizen $P\ P^2\ P^3 \dots P^k \dots$ gleich 0 ist.

(wir wissen: $p_{ij}^{(k)} = (P^k)_{ij}$)

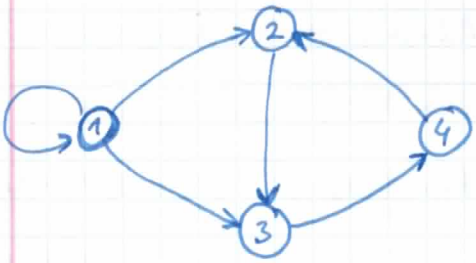
$p_{ij}^{(k)}$: Übergangswahrscheinlichkeit in k Schritten

$(P^k)_{ij}$: Übergangsmatrix hoch k

MK 16.

- eine reduzible Markoff-Kette wird langfristig in eine starke Zusammenhangskomponente absorbiert wobei diese Zusammenhangskomponente von Außen nur eingehende Kanten hat. (absorbierende starke Zusammenhangskomponente)
- Welche sind die starken Zusammenhangskomponenten in unserem G?

2.) Periodische Knoten



Was kann man über das langfristige Verhalten dieser Markoff-Kette vorhersagen?

→ {2, 3, 4} ist eine absorbierende starke Zusammenhangskomponente

→ Wenn die Markoff-Kette in einem der Zustände {2, 3, 4} gerät, danach verhält sie sich periodisch.

⇒ die Knoten 2, 3, 4 sind alle sogenannte periodische Knoten mit Periode 3.

Wie könnte man die Periodizität eines Knotens i mit Hilfe der Übergangswahrscheinlichkeiten $p_{ii}^{(k)}$ formal definieren?

Im Beispiel oben für i = 2

$$p_{22} = 0 \quad p_{22}^{(2)} = 0 \quad p_{22}^{(3)} = 1 \quad p_{22}^{(4)} = 0 \quad p_{22}^{(5)} = 0 \quad p_{22}^{(6)} = 1$$

Definition: Ein Knoten i heißt **periodisch**, wenn eine $\Delta > 1$ existiert, so dass $p_{ii}^{(k)} > 0 \Rightarrow \Delta \mid k$ (Δ teilt k). Die größte solche Δ ist die **Periode** des Knotens.

(Anders: die Periode von i $= ggt \{ k \mid p_{ii}^{(k)} > 0 \}$

3.) Periodische Markoff-Ketten

Definition: eine Markoff-Kette ist **periodisch** wenn sie mindestens einen periodischen Knoten hat, und **aperiodisch** sonst.

Wir werden sehen: in einer **irreduziblen** Markoff-Kette sind entweder **alle** Knoten periodisch, oder **alle** aperiodisch.

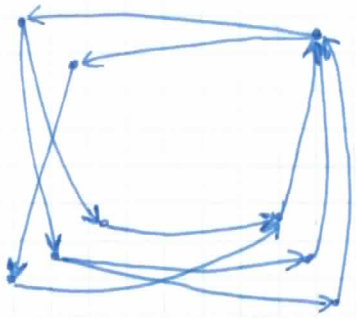
Eine periodische Markoff-Kette hat also immer wieder 0-Einträge $p_{ii}^{(k)}$ in den Matrizen

$$P, P^2, P^3, \ldots P^k \ldots$$

MK18.

Wie sieht eine ireduzible (stark zusammenhängende) periodische Markoff-Kette aus?

→ Entwerfen wir eine ireduzible Markoff-Kette mit 9 Knoten, und Periode 4 für jeden Knoten



bei jeder periodischen Markoff-Kette gibt es eine solche Zerlegung der Knotenmenge in Δ Mengen

Bei ireduziblen Ketten:

→ Wäre es möglich, dass manche Knoten periodisch, manche aperiodisch sind?

→ Wäre es möglich dass ein Knoten in einer periodischen Kette Eigenschleife hat? Oder dass zwei Knoten unterschiedliche Perioden haben?

Theorem: In einer ireduziblen periodischen Markoff-Kette hat jeder Knoten die gleiche Periode.

Beispiel: Im 2-SAT haben wir diese Markoff-Kette definiert:

Ist sie ireduzibel? NEIN

Ist sie periodisch? ~~JA~~ ~~NEIN~~ 0-(n-1) periodisch (n aperiodisch)

Was wäre die Antwort mit der Kante $(n, n-1)$ statt (n, n)?

MK 19.

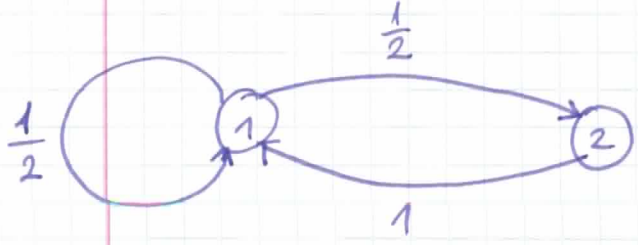
4. Ergodische Markoff-Ketten

(Wir werden sehen: es handelt sich hier eigentlich um die irreduziblen und aperiodischen Markoff-Ketten)

Wenn die Kette reduzibel oder/und periodisch ist, dann wissen wir schon etwas über ihr langfristiges Verhalten. Wir werden Näheres wissen, wenn wir ergodische Markoff-Ketten kennen lernen.

a.) Intuitive Erklärung

Beispiel:



Übergangsmatrix

$$P = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ 1 & 0 \end{bmatrix}$$

- diese M.K. ist irreduzibel und aperiodisch
  (eine irreduzible Markoff-Kette mit mind. einer Eigenschleife ist nie periodisch)

→ Angenommen, die Startverteilung ist $\left(\frac{1}{2}, \frac{1}{2}\right)$,
in welchem Zustand befindet sich diese Markoff-Kette häufiger langfristig (und um wieviel häufiger)?

→ Es geht darum, dass wir vermuten, dass über 100000 Schritte die M.K. etwa $\pi_1 \cdot 100000$ mal im Zustand ① und etwa $\pi_2 \cdot 100000$ mal im Zustand ② ist, für irgendwelche $\pi_1 + \pi_2 = 1$

→ Anders gesagt: wenn wir nach 100000 Schritten den aktuellen Zustand betrachten / vorhersagen würden, würden wir erwarten, dass die M. K. mit bestimmter Wahrscheinlichkeit $\approx \pi_1$ im Zustand ①, und mit Wahrscheinlichkeit $\approx \pi_2 = 1 - \pi_1$ im Zustand ② ist

→ Andererseits, können wir die Wahrscheinlichkeiten nach $t = 100000$ Schritten genau berechnen!
Für Startverteilung $q = \left(\frac{1}{2}, \frac{1}{2}\right)$ bezeichne

$q_1^{(t)} = P_{q_0}(X_t = 1)$ und $q_2^{(t)} = P_{q_0}(X_t = 2)$ die genaue Verteilung nach t Schritten. Wir wissen: für $t = 100000$

$$(q_1\ q_2) \cdot P^{100000} = (q_1, q_2) \cdot \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ 1 & 0 \end{bmatrix}^{100000} = (q_1^{(t)}, q_2^{(t)}) \approx (\pi_1, \pi_2)$$

→ (Angenommen, dass $q_1^{(t)} \approx \pi_1$ und $q_2^{(t)} \approx \pi_2$ für irgendeine Verteilung (π_1, π_2) und t groß genug, so könnten wir durch $q \cdot P^t$ die π_1 und π_2 schätzen; wir werden stattdessen (π_1, π_2) mit einer anderen Methode genau berechnen, aber wir formulieren unsere Annahme über π_1, π_2 präziser:)

→ Wenn wir eine gute Schätzung π_1, π_2 für die Verteilung im Schritt $t = 100000$ hätten, dann wäre unsere Schätzung für die Verteilung in $t+1 = 100001$ dieselbe (da die Kette aperiodisch, und wir die Schritte $1, 2, 3, \ldots, 100000, 100001$ nicht kennen)
(Wenn unser Freund über einen späten Zustand der M.K. wetten möchte, es ist egal, ob er $t = 100000$, oder 100001 erwähnt.)

Das heisst, wir vermuten nicht nur $q_1^{(t)} \approx \pi_1$ $q_2^{(t)} \approx \pi_2$ aber auch $q_1^{(t+1)} \approx \pi_1$ $q_2^{(t+1)} \approx \pi_2$ für t hoch genug.

Wir formulieren eine noch stärkere intuitive Vermutung, und halten uns daran (kein Beweis!):

Ausgangspunkt:

Wir nehmen an, dass die Grenzwerte π_1 π_2 existieren (für unsere Markoff-Kette), so dass

$$q_1^{(t)} \longrightarrow \pi_1 \text{ und } q_2^{(t)} \longrightarrow \pi_2 \text{ wenn } t \to \infty.$$

→ In diesem Fall gilt natürlich auch

$$q_1^{(t+1)} \longrightarrow \pi_1 \text{ und } q_2^{(t+1)} \longrightarrow \pi_2 \text{ wenn } t \to \infty$$

Wir wissen aber, um einen Schritt weiter die Verteilung zu berechnen:

$$\left[q_1^{(t)}, q_2^{(t)}\right] \cdot \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ 1 & 0 \end{pmatrix} = \left[q_1^{(t+1)}, q_2^{(t+1)}\right]$$

also:

$$\pi_1 \longleftarrow q_1^{(t+1)} = q_1^{(t)} \cdot \frac{1}{2} + q_2^{(t)} \cdot 1 \longrightarrow \pi_1 \cdot \frac{1}{2} + \pi_2 \cdot 1$$

$$q_2^{(t+1)} = q_1^{(t)} \cdot \frac{1}{2} + q_2^{(t)} \cdot 0$$

Da der erste Term einerseits gegen π_1, andererseits gegen $\pi_1 \cdot \frac{1}{2} + \pi_2 \cdot 1$ konvergiert, jedoch nur einen Grenzwert besitzen kann (höchstens), es muss gelten, dass

$$\pi_1 = \pi_1 \cdot \frac{1}{2} + \pi_2 \cdot 1$$

und analog

$$\pi_2 = \pi_1 \cdot \frac{1}{2} + \pi_2 \cdot 0$$

Die beiden Gleichungen sind äquivalent, aber wir haben noch die Forderung

$$\Pi_1 + \Pi_2 = 1$$

und so erhalten wir die Grenzverteilung $\Pi_1 = \frac{2}{3}$ $\Pi_2 = \frac{1}{3}$

→ Wir haben erhalten:

Angenommen, dass die Wahrscheinlichkeitsverteilung $(q_1^{(t)}\ q_2^{(t)} \dots q_n^{(t)})$ für eine Startverteilung q zu einer Grenzverteilung $(\Pi_1 \Pi_2 \dots \Pi_n)$ konvergiert (d.h. jeder Eintrag $q_i^{(t)} \to \Pi_i$ konvergiert), dann gilt

$$\Pi \cdot P = \Pi \quad \text{für den Zeilenvektor } \Pi.$$

$$\{\Pi_1 \Pi_2 \dots \Pi_n\} \begin{pmatrix} p_{11} & \dots & p_{1n} \\ \vdots & & \\ p_{n1} & \dots & p_{nn} \end{pmatrix} = \{\Pi_1 \Pi_2 \dots \Pi_n\}$$

d.h. Π ist eine sog. stationäre Verteilung für die Markoff-Kette P.

→ Würden wir die relative Häufigkeit der Zustände in unserer M.K. anders abschätzen, wenn die Startverteilung nicht $q = (\frac{1}{2}, \frac{1}{2})$ wäre?

Intuition: Da die M.K. aperiodisch und irreduzibel (stark zusammenhängend) ist, beeinflusst die Startverteilung das langfristige Verhalten mit wachsender t immer weniger. Wir präzisieren unsere Annahme dementsprechend (kein Beweis):

Wir nehmen an, dass die Grenzverteilung Π existiert, und ist unabhängig von der Startverteilung (für irred. und aperiodische M.K.), d.h. $q_i^{(t)} \to \Pi_i$ wenn $t \to \infty$ für beliebige $q = q^{(0)}$.

MK 23. → Wir betrachten jetzt die Potenzen P^t der Übergangsmatrix. Wir haben angenommen, dass für beliebige Startverteilung (q_1, q_2)

$$(q_1, q_2) \cdot P^t = (q_1\ q_2) \cdot \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ 1 & 0 \end{pmatrix}^t = (q_1^{(t)}, q_2^{(t)}) \to (\pi_1, \pi_2)$$

Wie kann P^t aussehen?

Sei z.B. $q = (1, 0, 0, \ldots, 0)$ die Startverteilung. Dann ist $q \cdot P^t$ die erste Zeile von P^t. Andererseits $q \cdot P^t \to \pi$ wenn $t \to \infty$. D.h. die erste Zeile von P^t geht gegen den Zeilenvektor π (für jede Koordinate), als $t \to \infty$.

Wenn wir $q = (0, 0, 0, \ldots 0, \underset{i}{1}, 0, \ldots, 0)$ für $i = 1, 2, \ldots, n$ einsetzen, erhalten wir, dass jede Zeile der Potenzmatrix P^t zu der Grenzverteilung π konvergieren soll! Wir haben erhalten:

P^t konvergiert zu einer Matrix P^∞, (wenn $t \to \infty$), so dass jede Zeile von P^∞ die Grenzverteilung $\pi = (\pi_1, \pi_2 \ldots \pi_n)$ ist

$$P^\infty = \begin{pmatrix} \pi_1 & \pi_2 & \ldots & \pi_n \\ \pi_1 & \pi_2 & \ldots & \pi_n \\ \vdots & & & \\ \pi_1 & \pi_2 & \ldots & \pi_n \end{pmatrix}$$

Für beliebige Verteilung q gilt

$$\boxed{q \cdot P^\infty = \pi}$$

weil

$$[q_1\, q_2 \dots q_n] \cdot \begin{pmatrix} \pi_1 & \pi_2 & \dots & \pi_n \\ \pi_1 & \pi_2 & \dots & \pi_n \\ \vdots & & & \\ \pi_1 & \pi_2 & \dots & \pi_n \end{pmatrix} = \left[\pi_1 \underbrace{\sum_i q_i}_{=1}, \pi_2 \underbrace{\sum_i q_i}_{=1}, \dots, \pi_n \sum_i q_i\right] =$$

$$= [\pi_1\ \pi_2 \dots \pi_n]$$

Die folgenden Beobachtungen sind intuitiv klar:

- für eine (starke zusammenhängende) periodische Kette kann eine Grenzverteilung nicht existieren: die Werte $p_{ii}^{(t)}$ sind manchmal 0, manchmal $> c$ für eine positive c.

- für einen Graphen, der nicht stark zusammenhängend ist (die Markoff-Kette ist reduzibel), wären manche Grenzwerte in P^t gleich 0.
  Wenn es mehrere absorbierende Zusammenhangskomponenten gibt, dann wären ihre Grenzverteilungen von der Startverteilung abhängig.

- „Umgekehrt" gilt aber auch: Wenn die Markoff-Kette irreduzibel ist, und die Grenzverteilung Π existiert, dann sind die Wahrscheinlichkeiten π_i der Zustände alle positiv: es ist nicht möglich eine (endliche) stark zusammenhängende Markoff-Kette zu konstruieren, so dass ein Knoten langfristig mit Wahrscheinlichkeit 0 besucht wird.

b.) Formale Definitionen: (der Einfachheit halber wird hier von der anderen Richtung aus definiert)

Def: Die Markoff-Kette (G, P) heißt ergodisch, wenn für alle i_1, i_2, j die positiven Grenzwerte

$$\lim_{t\to\infty} p^t_{i_1 j} > 0 \text{ und } \lim_{t\to\infty} p^t_{i_2 j} > 0 \quad \text{(Einträge in } P^t\text{)}$$

existieren und gleich sind. Die Verteilung

$$\pi_j^\infty = \lim_{t\to\infty} p^t_{1j} \quad (\text{für } j = 1, 2, \dots, n)$$

heißt die Grenzverteilung von (G, P)

Folglich: → Für eine ergodische Markoff-Kette ist die Matrix $\boxed{P^\infty = \lim_{t\to\infty} P^t}$ wohldefiniert, und

→ jede Zeile von P^∞ ist die Grenzverteilung π^∞,

→ und für beliebige Startverteilung q gilt $\boxed{q \cdot P^\infty = \pi^\infty}$

→ damit gilt auch für π^∞ $\boxed{\pi^\infty \cdot P^\infty = \pi^\infty}$

$$P^t = \begin{matrix} \\ i_1) \\ i_2) \end{matrix} \begin{matrix} \overset{j}{} \end{matrix} \begin{bmatrix} & p^{(t)}_{1j} & \\ & p^{(t)}_{i_1 j} & \\ & p^{(t)}_{i_2 j} & \end{bmatrix} \longrightarrow \begin{bmatrix} \overset{j}{} \\ \pi_j^\infty \\ \pi_j^\infty \\ \pi_j^\infty \end{bmatrix}$$

MK 26.

Definition: Eine Verteilung π' heißt stationäre Verteilung, wenn (für den Zeilenvektor π') gilt $\pi' \cdot P = \pi'$

Theorem: Für jede ergodische Markoff-Kette ist ihre Grenzverteilung π^∞ die einzige stationäre Verteilung.

Beweis:

→ π^∞ ist stationär:

es gilt $p^t \cdot P = p^{t+1}$ — wenn $t \to \infty$

die Einträge konvergieren: $p^\infty \cdot P = p^\infty$

das Produkt konvergiert zu diesem Produkt

deshalb besteht Gleichheit $p^\infty \cdot P = p^\infty$

$\Rightarrow \pi^\infty \cdot p^\infty \cdot P = \pi^\infty \cdot p^\infty$

weil $q \cdot p^\infty = \pi^\infty$ gilt für jeden q ← $\pi^\infty \cdot P = \pi^\infty$ → siehe oben

$\Rightarrow \pi^\infty$ ist stationär

→ π^∞ ist die einzige:

Angenommen, π' wäre eine andere stationäre Verteilung, dann

$$\pi' = \pi' \cdot P = \pi' \cdot P \cdot P = \dots = \pi' \cdot p^t = \pi' p^\infty = \pi^\infty$$

- $\pi' = \pi' \cdot P$: weil π' stationär
- $= \pi' \cdot P \cdot P$: wiederholt
- $= \pi' \cdot p^t$: $\pi' \cdot p^\infty$
- $= \pi' p^\infty$: weil konstante Folge $\pi' \cdot p^t$ konvergiert zu $\pi' p^\infty$
- $= \pi^\infty$: weil $q \cdot p^\infty = \pi^\infty$ für jede q

Beobachtung: Da Π^∞ die einzige Verteilung ist, die $\Pi^\infty \cdot P = \Pi^\infty$ erfüllt (bei ergodischen Ketten!), um Π^∞ zu berechnen, braucht man nur das Gleichungssystem

$$\Pi = \Pi \cdot P$$

mit der zusätzlichen Gleichung

$$\sum_{i=1}^{n} \Pi_i = 1$$

für die Unbekannten $\Pi = (\Pi_1, \Pi_2, \Pi_3, \ldots, \Pi_n)$ zu lösen.

Theorem: Eine Markoff-Kette ist ergodisch

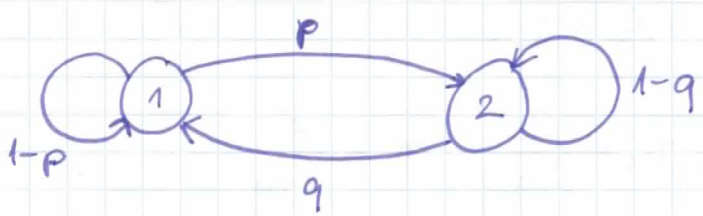
$\Downarrow\Uparrow$

sie ist irreduzibel und aperiodisch

($\Downarrow$) trivial, sonst können überall positive Grenzwerte für die Matrizen P^t ($t \to \infty$) nicht existieren, da die Matrix-Einträge in P^t für unendlich viele t 0 sind.

($\Uparrow$) ohne Beweis

Beispiel: Für welche p, q Werte ist die folgende Markoff-Kette ergodisch?



$$P = \begin{bmatrix} 1-p & p \\ q & 1-q \end{bmatrix}$$

MK28.

→ Wir prüfen

- für welche p, q ist sie irreduzibel?

für $p=0$ <u>oder</u> $q=0$ nicht

$\Rightarrow$ $p>0$ und $q>0$ sind notwendig

- für welche p, q ist sie aperiodisch?

für $p=1$ <u>und</u> $q=1$ nicht

$\Rightarrow$ $p<1$ <u>oder</u> $q<1$ ist notwendig

Für solche p und q ist die M.K. irreduzibel und aperiodisch und deshalb ergodisch.

→ die Lösung des Gleichungssystems

$$\pi \cdot P = \pi \longrightarrow (\pi_1, \pi_2)\begin{pmatrix} 1-p & p \\ q & 1-q \end{pmatrix} = (\pi_1, \pi_2)$$

$$\pi_1 + \pi_2 = 1$$

ist die Grenzverteilung

Das Gleichungssystem:

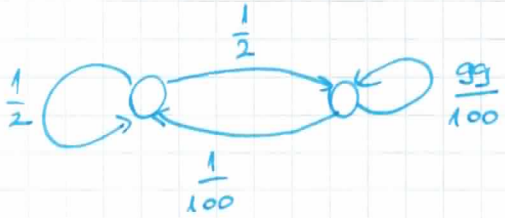
(1) $(1-p)\cdot\pi_1 + q\pi_2 = \pi_1 \Rightarrow q\cdot\pi_2 = p\cdot\pi_1$

($p\cdot\pi_1 + (1-q)\cdot\pi_2 = \pi_2 \Rightarrow p\cdot\pi_2 = q\cdot\pi_2$ dasselbe)

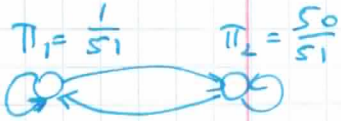
(2) $\pi_1 + \pi_2 = 1$

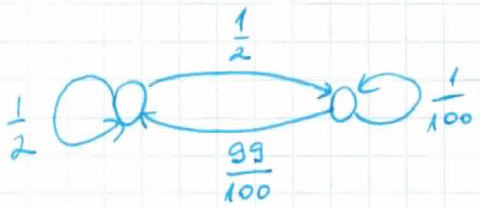
(1) + (2) ergibt $\pi_1 = \frac{q}{p+q}$ $\pi_2 = \frac{p}{p+q}$

Bemerkung: Für die Beispiele



erhalten wir





erhalten wir

Beispiel: Random Walks in ungerichteten Graphen

1.) Definition

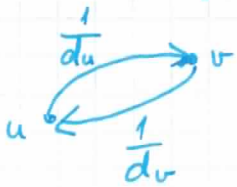
Wir wollen einen (zusammenhängenden?) ungerichteten Eingabegraphen zufällig durchlaufen entdecken. Aus den aktuellen Nachbarknoten wird immer gleichverteilt einer ausgewählt. Wir betrachten jetzt die Eigenschaften dieses Random Walks:

Sei $G(V,E)$ ein beliebiger ungerichteter Graph (ohne isolierte Knoten). Wir definieren eine Markoff-Kette auf den Knoten V als Zuständen, und Übergangswahrscheinlichkeiten

$$p_{uv} = \begin{cases} \frac{1}{d_u} & \text{falls } \{u,v\} \in E \text{ und } d_u = \text{Grad}(u) \\ 0 & \text{falls } \{u,v\} \notin E \end{cases}$$

MK 30.

In der Markoff-Kette wird also jede ungerichtete Kante $\{u, v\}$ durch 2 gerichteten Kanten ersetzt.



aus einer Eigenschleife werden 2 Kanten

um die Analyse zu erleichtern.

2. Wann ist diese Markoff-Kette irreduzibel/aperiodisch/ergodisch?

irreduzibel → immer (zumindest innerhalb jeder einzelner Zusammenhangskomponente): wir können von jedem Knoten u zu jedem Knoten v laufen.

periodizität Kann ein Random Walk auf einem ungerichteten Graphen periodisch sein? (Wenn ja, dann hat jeder Knoten die selbe Periode)
Betrachte einen einfachen Weg (starte in ⓪)

→ in jedem Zweiten Schritt ist die Kette in geradem Zustand

→ wir haben hier nämlich mit einem bipartiten Graphen zu tun.

→ Wenn der ungerichtete Graph G bipartit ist, dann hat die entsprechende Markoff-Kette die Periode 2;
(Warum kann die Periode nicht 4, 6, 8... sein?)

→ wenn G nicht bipartit ist, dann hat er mindestens einen ungeraden Kreis, und natürlich auch Kreise der Länge 2 (Warum?), wie jeder Graph. Es gibt keine mögliche Periode $\Delta > 0$, die sowohl 2 als auch die ungerade Kreislänge teilt.

Thm: Wenn G nicht bipartit ist, dann ist die Markoff-Kette auf G aperiodisch und irreduzibel, und damit ergodisch.

Im Folgenden nehmen wir an, dass G nicht-bipartit, und damit ergodisch ist. (Dies können wir mit der Hinzunahme einer Eigenschleife immer erreichen.)

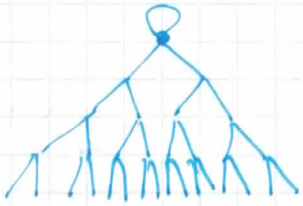
3. Die Grenzverteilung

Beispiel: Wir stellen uns verschiedene Graphen vor, und versuchen abzuschätzen, wie häufig sich die Kette in den einzelnen Zuständen befindet, also praktisch die Grenzverteilung (die Position der Eigenschleife ist in jedem Graph unwichtig.) π.

ein Weg

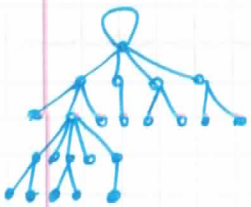
ein Stern

(ungerader) Kreis



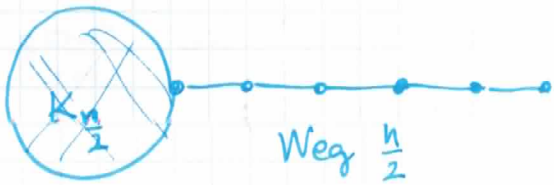
Binärbaum

MK 32.



Baum

der Lollipop-Graph



Theorem: Die Grenzverteilung des Random Walks auf G ist

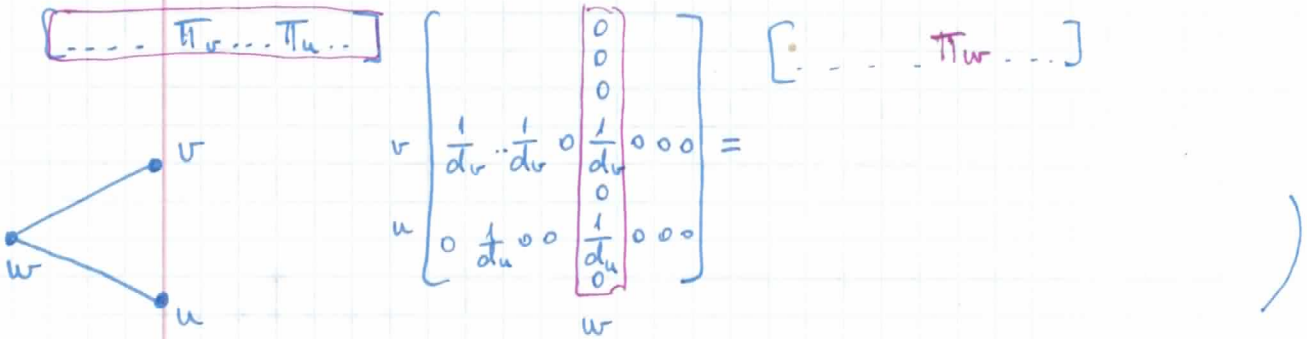
$$\boxed{\pi_v = \frac{d_v}{2|E|} \qquad (v \in V)}$$

Das heißt, die Wahrscheinlichkeit eines beliebigen Knotens ist proportional mit $d_v = \text{Grad}(v)$

Prüfe: Ist diese eine Verteilung? $\sum_v \frac{d_v}{2|E|} = \frac{1}{2|E|} \cdot \sum_v d_v = \frac{1}{2|E|} \cdot 2|E| = 1$

Beweis des Theorems:

Wir zeigen, dass diese $(\pi_v)_{v \in V}$ eine stationäre Verteilung ist. Da die Grenzverteilung in ergodischen Ketten die eindeutig bestimmte stationäre Verteilung ist, wird der Beweis damit erbracht. (Seien z.B. v und u die Nachbarn von w, und er habe keine andere Nachbarn.



Der Eintrag auf Position w im Produktvektor ist

$$\sum_{\{v \mid \{v,w\} \in E\}} \pi_v \cdot \frac{1}{d_v} = \sum_{\{v \mid \{v,w\} \in E\}} \frac{d_v}{2|E|} \cdot \frac{1}{d_v} = \frac{1}{2|E|} \cdot \sum_{\{v \mid \{v,w\} \in E\}} 1 = \frac{d_w}{2|E|} = \pi_w$$

□

5. Wir berechnen noch zwei Erwartungswerte

Definition: Für beliebige zwei Knoten $u, v \in V$, sei h_{uv} die erwartete Anzahl der Schritte bis v zum ersten mal erreicht wird, wenn der Walk in u startet.

→ Wir schätzen h_{uu} ab (intuitiv):

Wir kennen die Wahrscheinlichkeit π_u und damit die (erwartete) relative Häufigkeit (Anteil / Bruchteil) aller Schritte in denen die Markoff-Kette im Zustand u ist.

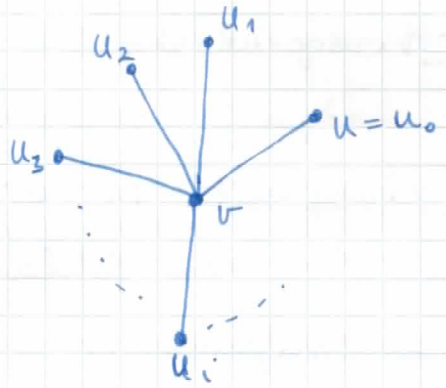
- Wenn $\pi_u = \frac{1}{3}$, dann wird der Random Walk etwa alle drei Schritte immer wieder in u sein.

  Gefühlt: $h_{uu} = 3$

- Wenn $\pi_u = \frac{1}{10}$, dann $h_{uu} = 10$
- Wenn $\pi_u = \frac{3}{4}$, dann $h_{uu} = \frac{4}{3}$

$$\boxed{h_{uu} = \frac{1}{\pi_u} = \frac{2|E|}{d_u}}$$

→ sei $\{u, v\} \in E$; wir schätzen h_{uv} nach oben ab (also nur im Fall, wenn $\{u\ v)$ eine Kante ist)



wir wissen: $h_{vv} = \frac{2|E|}{d_v}$ (1)

es gilt auch: $h_{vv} = \sum_{u_i \in N(v)} \frac{1}{d_v} \cdot (1 + h_{u_i v})$ (2)

Erwartungswert, je nachdem wohin der erste Schritt aus v führt.

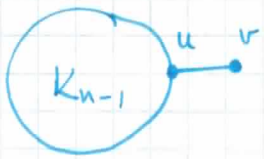
Aus (1) + (2):

$$\sum_{u_i \in N(v)} (1 + h_{u_i v}) = 2|E|$$

$\Rightarrow$ also $h_{uv} < 2|E|$ für jeden Nachbarn von v

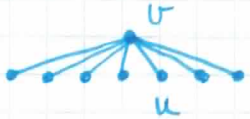
$\boxed{h_{uv} < 2|E|}$ für eine beliebige Kante $\{u,v\} \in E$

(Im Allgemeinen ist $h_{uv} \neq h_{vu}$



$h_{vu} = 1$

$h_{uv} = ?$



$h_{uv} = 1$

$h_{vu} = ?$

Beispiel: das 3-SAT Problem

- im 3-SAT Problem hat in der Eingabe jede Klausel ≤ 3 **Literale**.

3-SAT ist ein NP-vollständiges Problem!
Was kann man hier überhaupt hoffen?

→ Einen deterministischen Algorithmus mit polynomieller Laufzeit zu finden, würde also P=NP implizieren... (diese Möglichkeit schliessen wir jetzt aus).

→ Für schwierige Probleme ist auch die Existenz eines randomisierten Algorithmus mit polynomieller (erwarteten) Laufzeit praktisch ausgeschlossen (es würde ähnlich überraschende Folgen haben komplexitätstheoretisch).

→ Bei Monte Carlo Algorithmen ist die Laufzeit (z.B. Anzahl der Iterationen) meistens festgelegt. (worst case)
Bei Las Vegas Algorithmen rechnet man mit der erwarteten Laufzeit. Die obige Bemerkung betrifft beide.

Auch mit dem Random Walk Algorithmus für 3-SAT werden wir (anders als bei 2-SAT) exponentielle Laufzeit erwarten.
Wir beobachten jetzt die entscheidenden Unterschiede zur Analyse von 2-SAT.

— der Random Walk Algorithmus für 2-SAT hätte in diesem Fall die folgende Analyse:

der Algorithmus:

- wähle eine Belegung b (Wahrheitswerte) zufällig

WIEDERHOLE
- FALLS b erfüllt die Eingabeformel, return b;
- SONST sei k_e eine beliebige unerfüllte Klausel, wähle eine Variable von k_e zufällig und flippe ihren Wahrheitswert;

→ Wir nehmen an, dass eine erfüllende Belegung S existiert, und definieren die Zustände

0, 1, 2, 3, ..., n-1, n

als die Anzahl der Variablen, die im aktuellen b Wahrheitsbelegung den gleichen Wert haben wie in S.

Wir geben eine pessimistische Abschätzung für die Übergangswahrscheinlichkeiten:

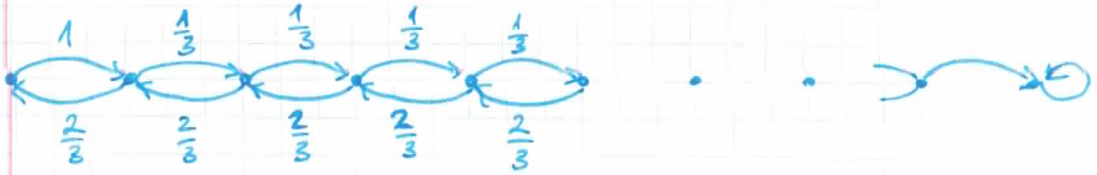
Sei z.B. $x_1 \vee \bar{x}_2 \vee x_3$ die unerfüllte Klausel in b

dann gilt $x_1 = 0$, $x_2 = 1$, $x_3 = 0$ in b

und $x_1 = 1$ oder $x_2 = 0$ oder $x_3 = 1$ (bzw. mehrere davon) in S

der Random Walk hat $\geq \frac{1}{3}$ Wahrscheinlichkeit ($\frac{1}{3}$, $\frac{2}{3}$ oder 1) eine solche Variable zu flippen, und damit einen Schritt nach rechts ($j \longrightarrow j+1$) zu laufen;

ebenfalls, er hat $\leq \frac{2}{3}$ Wahrscheinlichkeit in die falsche Richtung zu laufen. Wir erhalten die pessimistische (worst case) Markoff-Kette:



Sei h_j die erwartete Anzahl der nötigen Schritte in dieser M.K. bis der Random Walk vom Zustand j zum Zustand n kommt. Es gelten:

$$h_n = 0$$

$$h_0 = 1 + h_1$$

$$h_j = 1 + \frac{1}{3} \cdot h_{j+1} + \frac{2}{3} h_{j-1} \qquad j = 1, \ldots, n-1$$

Man kann zeigen mit Induktion:

$$h_j = h_{j+1} + 2^{j+2} - 3$$

und damit

$$h_0 = h_1 + 2^2 - 3 =$$

$$= h_2 + 2^3 + 2^2 - 2 \cdot 3 =$$

$$\vdots$$

$$= h_n + 2^{n+1} + 2^n + 2^{n-1} + \ldots + 2^2 - n \cdot 3 = 2^{n+2} - 1 - (n+1) \cdot 3$$

$\Rightarrow$ für 3-SAT wäre so ein Random Walk noch schlimmer als alle 2^n Wahrheitsbelegungen deterministisch zu testen.

Der Random Walk geht mit höherer Wahrscheinlichkeit in die falsche Richtung (im Gegensatz zu 2-SAT)! Auch wenn die Anfangsbelegung b ganz gut war, falls S nicht schon am Anfang gefunden wurde, wird sich

der Random Walk immer mehr in niederwertigen Zuständen herumirren. Je länger der Random Walk, desto weniger zählt, was die Anfangsbelegung war.

Was ist also der Ausweg für 3-SAT?

→ Starte den Random Walk immer wieder neu: nach relativ kurzem Random Walk wähle wieder eine Anfangsbelegung zufällig:

Der Algorithmus für 3-SAT

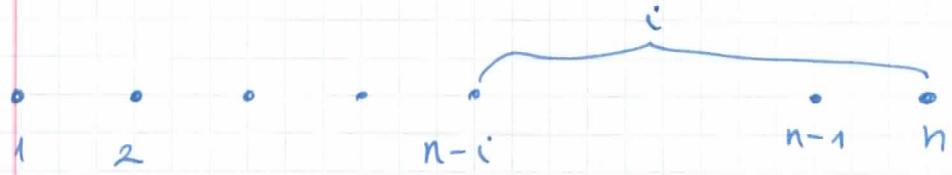
```
WIEDERHOLE  m-mal
    1. wähle eine zufällige Belegung b
    2. WIEDERHOLE 3n-mal
        2.a. FALLS b die Formel erfüllt, return b;
        2.b. SONST flippe den Wert einer
             zufällig gewählter Variable einer
             beliebigen unerfüllten Klausel, und
             sei b diese neue Belegung;
GIB „nicht-erfüllbar" aus;
```

Skizze der Analyse (aus Mitzenmacher-Upfal)

Sei S eine fixierte erfüllende Belegung, und b die zufällige Startbelegung. Wir berechnen

Prob (Erfolg (S finden) in 3n Schritten)

MK 60.



Erfolgswahrscheinlichkeit $\geq \frac{c}{\sqrt{i}} \cdot \frac{1}{2^i}$

Behauptung: Sei $n-i$ der Anfangszustand, d.h. S und b unterscheiden sich in genau i Wahrheitswerten für $i>0$. Die Wahrscheinlichkeit, dass der Random Walk in $3n$ Schritten die Belegung S findet, ist mindestens

$$\frac{c}{\sqrt{i}} \cdot \frac{1}{2^i} \geq \frac{c}{\sqrt{n}} \cdot \frac{1}{2^i} \qquad \left(c = \frac{\sqrt{3}}{8\sqrt{\pi}}\right)$$

(ohne Beweis)

Die Belegung b wird zufällig gewählt, so dass jede Variable mit Wahrscheinlichkeit $\frac{1}{2}$ auf 0 bzw. auf 1 gesetzt wird. Wie hoch ist die Wahrscheinlichkeit, dass S und b sich in genau i Werten unterscheiden?

$$\binom{n}{i} \cdot \left(\frac{1}{2}\right)^n$$

(Es gibt $\binom{n}{i}$ mögliche Mengen von i Variablen, wo b und S unterschiedlich sind. Wenn wir eine solche Menge von i Variablen festlegen, bestimmt das die Belegung relativ zu S eindeutig: die Wahrscheinlichkeit dieser konkreten Belegung ist $\left(\frac{1}{2}\right)^n$.)

Wir berechnen jetzt die Wahrscheinlichkeit, dass mit einer zufälligen Belegung angefangen, der Random Walk in $3n$ Schritten die Belegung S findet:

$$\text{Prob}\left(S \text{ finden in } 3n \text{ Schritten}\right) = \sum_{i=0}^{n} P(i \text{ Unterschiede}) \cdot P\left(S \text{ finden in } 3n \,\middle|\, \substack{i \\ \text{Unter-} \\ \text{schiede}}\right)$$

$P(i \text{ Unterschiede}) \rightarrow \binom{n}{i}\left(\frac{1}{2}\right)^n$

$P\left(S \text{ finden in } 3n \,\middle|\, i \text{ Unterschiede}\right) = \frac{c}{\sqrt{n}} \cdot \frac{1}{2^i}$

$$\geq \underbrace{\frac{1}{2^n}}_{\text{kein Unterschied}} + \sum_{i=1}^{n} \binom{n}{i}\left(\frac{1}{2}\right)^n \cdot \frac{c}{\sqrt{n}} \cdot \frac{1}{2^i} \geq \frac{c}{\sqrt{n}} \cdot \left(\frac{1}{2}\right)^n \cdot \sum_{i=0}^{n} \binom{n}{i}\left(\frac{1}{2}\right)^i =$$

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

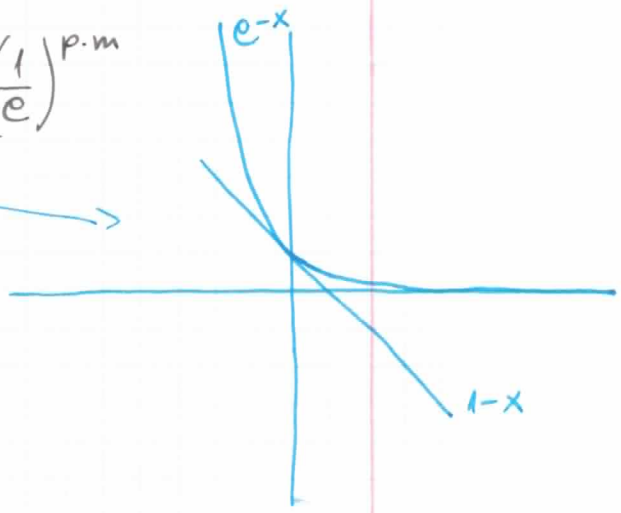
binomischer Lehrsatz

$$= \frac{c}{\sqrt{n}} \cdot \left(\frac{1}{2}\right)^n \cdot \left(\frac{3}{2}\right)^n = \frac{c}{\sqrt{n}} \cdot \left(\frac{3}{4}\right)^n$$

$\Rightarrow$ in jeder Runde der äusseren Schleife hat der Algorithmus Erfolgswahrscheinlichkeit mindestens $p \geq \frac{c}{\sqrt{n}} \cdot \left(\frac{3}{4}\right)^n$

$\rightarrow$ die Fehlerwahrscheinlichkeit nach den m Runden:

$$\leq (1-p)^m \leq e^{-pm} = \left(\frac{1}{e}\right)^{p \cdot m}$$



MK 62.

Sei $L = m \cdot p$, dann hat der Algorithmus

$$\boxed{\text{Fehlerwahrscheinlichkeit} \leq \left(\frac{1}{e}\right)^L}$$

und

$$\boxed{\text{Laufzeit} \leq 3nm = 3n \cdot \frac{L}{p} = \frac{3n \cdot \sqrt{n} \cdot L}{c} \cdot \left(\frac{4}{3}\right)^n}$$

→ in L lineare Laufzeit, exponentielle Fehlerwahrscheinl.
in n exponentiell, aber mit Basis $\frac{4}{3} = 1,3333..$ (statt 2)

Im Skript wird noch ein deterministischer Algorithmus mit Laufzeit $\text{poly}(n, N) \cdot \mathcal{O}\left(7^{\frac{n}{3}}\right) =$

$\text{poly}(n, N)\, \mathcal{O}\left(1,913^n\right)$ präsentiert.