Lehr- und Forschungsgebiet der Theoretischen Informatik
RWTH Aachen

Ausarbeitung zum

# Seminar
# Extremal Combinatorics

bei Univ.-Prof. Dr. P. Rossmanith
im Sommersemester 2004

Thema
**Linearität des Erwartungswertes**
**Mark Walecki-Mingers**

# Inhaltsverzeichnis

# 1 Einleitung

In der Kombinatorik geht es oftmals um die Auswahl von Objekten, die gewisse Eigenschaften besitzen, und deren Anzahlen. Ein einfaches Abzählen ist nicht immer möglich. Mit Hilfe der Eigenschaft der Linearität des Erwartungswertes lassen sich Beweise von Existenzen von gesuchten Objekten im stochastischen Modell realisieren und elegant lösen. Dabei macht man sich zu Nutze, dass es eine Realisation eines Zufallsexperimentes geben muss, welche größer- bzw. kleiner gleich als der gewichtete Mittelwert aller Ereignisse ist, welcher oft einfach(er) zu berechnen ist. Dies nennt man die *Schubfacheigenschaft* der Erwartungswertes.
Um die Linearität ausnutzen zu können, ist es notwendig die gegebene Problemstellung in ein wahrscheinlichkeitstheoretisches Modell einzubetten. Dazu werden zunächst einige Grundbegriffe aus der Wahrscheinlichkeitstheorie definiert.

# 2 Der Erwartungswert

## 2.1 Stochastische Grundlagen

Damit die zu beweisenden Aussagen auch ihre Richtigkeit besitzen, muss alles auf das Fundament der Wahrscheinlichkeitstheorie gestellt werden. Alle zubehandelden Probleme erfordern nur diskrete Betrachtungen, daher genügt es, alle Definitionen auf den diskreten Raum zu beziehen.

**2.1 Definition** (Wahrscheinlichkeitsraum)
*Sei*

- $\Omega = \{\omega_1, \omega_1, \ldots\}$ *eine nichtleere abzählbare Menge*
- $\mathfrak{A} \subseteq \mathcal{P}(\Omega)$ *eine* $\sigma$*-Algebra über* $\Omega$*, d.h.*
  - $\emptyset \in \mathfrak{A}$
  - $A \in \mathfrak{A} \Rightarrow A^C \in \mathfrak{A}$
  - $(A_n)_{n\in\mathbb{N}}$ *ein Folge aus* $\mathfrak{A} \Rightarrow \bigcup_{n\in\mathbb{N}} A_n \in \mathfrak{A}$
- *ein Wahrscheinlichkeitsmaß* $Prob : \mathfrak{A} \to [0,1]$ *mit*
  - $Prob(\Omega) = 1$
  - $Prob(\bigcup_{n\in\mathbb{N}} A_n) = \sum_{n\in\mathbb{N}} Prob(A_n)\ \forall A_n \in \mathfrak{A}$ *paarweise disjunkt*

*gegeben. Dann ist das Tripel* $(\Omega, \mathfrak{A}, Prob)$ *ein* ***Wahrscheinlichkeitsraum****.*

**2.2 Definition** (Zufallsvariable)
*Sei* $(\Omega, \mathfrak{A}, Prob)$ *ein Wahrscheinlichkeitsraum. Eine Funktion* $X : \Omega \to \mathbb{R}$ *heißt* ***Zufallsvariable****, wenn* $X^{-1}(B) = \{\omega \in \Omega \mid X(\omega) \in B\} \in \mathfrak{A}\ \forall B \in \mathfrak{B}^1 (\mathfrak{B}^1$ *Borelsche Menge*$)$*. Durch* $Prob^X(B) = Prob(X^{-1}(B)) = Prob(\{\omega \in \Omega \mid X(\omega) \in B\})$ *wird eine Wahrscheinlichkeitsverteilung definiert.* $Prob^X$ *heißt* ***Verteilung*** *der Zufallsvariablen* $X$*.*
$X$ *bzw.* $Prob^X$ *heißen* ***diskret****, wenn eine höchstens abzählbare* ***Trägermenge*** $T = \{t_1, t_2, \ldots\}$ *existiert mit* $Prob^X(T) = 1$*.*

**2.3 Beispiel** *(i)* Indikatorfunktion
*Für* $A \subseteq \Omega$ *und* $x \in \Omega$ *sei*

$$\mathbb{1}_A(\{x\}) = \begin{cases} 1 & , x \in A \\ 0 & , x \notin A \end{cases}$$

*die* ***Indikatorfunktion****. Sie ist eine diskrete Zufallsvariable mit Träger $T = \{0, 1\}$, denn nach Definition gilt:* $\mathbb{1}_A^{-1}(1) = \{\omega \in \Omega \mid X(\omega) = 1\} = \{\omega \in A \mid X(\omega) = 1\} = A$

*(ii)* Binomialverteilung
*Ein Beispiel für die Binomialverteilung ist das stochastische Modell des n-fachen Münzwurfes. Dabei wird „Kopf" mit einer Wahrscheinlichkeit von $p$ und folglich „Zahl" mit $1-p$ angenommen.*
*Als Modell ergibt sich*

$$\Omega = \{\omega = \{x_1, \dots, x_n\} \mid x_i \in \{0,1\}\}$$
$$\mathfrak{A} = \mathcal{P}(\Omega)$$
$$Prob(\{x_1, \dots, x_n\}) = \overbrace{p \cdot \ldots \cdot p}^{Anzahl Einsen} \; \overbrace{(1-p) \cdot \ldots \cdot (1-p)}^{Anzahl Nullen} = p^{\sum_{i=1}^n x_i}(1-p)^{n-\sum_{i=1}^n x_i}$$

*Die möglichen Anzahlen von Einsen bildet die Trägermenge $T = \{0, 1, \dots, n\}$. Für die Zufallsvariable $X : \Omega \to T,\ X(\omega) = \sum_{i=1}^n x_i$ gilt*

$$\begin{aligned} Prob^X(\{k\}) &= Prob(X^{-1}(\{k\})) \\ &= Prob(\{\omega \mid X(\omega) = k\}) \\ &\overset{\text{kurz}}{=} Prob(X = k) \\ &= Prob(\{x_1, \dots, x_n\} \mid \textstyle\sum_{i=0}^n x_i = k\}) \\ &= \textstyle\sum_{\{x_1,\dots,x_n\}: \sum_{i=0}^n x_i = k} p^k(1-p)^{n-k} = \binom{n}{k} p^k (1-p)^{n-k} \end{aligned}$$

## 2.2 Definition des Erwartungswertes

Manchmal ist man nicht an der konkreten Wahrscheinlichkeit eines einzelnen Ereignisses interessiert, sondern an den durchschnittlichen Realisationen. Dabei sind die einzelnen Ereignisse mit der Wahrscheinlichkeit des Auftretens gewichtet.

**2.4 Definition** (Erwartungswert von Zufallsvariablen)
*Sei $X$ eine diskrete Zufallsvariable mit Träger $T = \{x_1, x_2, \dots\}$. Falls $\sum_{i=1}^\infty |x_i| P(X = x_i) < \infty$ existiert, so heißt $E[X] := \sum_{i=1}^\infty x_i P(X = x_i)$ der* ***Erwartungswert*** von $X$

**2.5 Beispiel** *(i)* Erwartungswert der Indikatorfunktion
*Sei $(\Omega, \mathfrak{A}, Prob)$ ein Wahrscheinlichkeitsraum, sowie $A \in \mathfrak{A}$*

$$\begin{aligned} E[X] &\overset{\text{Def.}}{=} \textstyle\sum_{\omega \in \Omega} \mathbb{1}_A(\omega) Prob(\{\omega\}) \\ &= \textstyle\sum_{\omega \in A} 1 \cdot Prob(\{\omega\}) + \sum_{\omega \in A^C} 0 \cdot Prob(\{\omega\}) \\ &= \textstyle\sum_{\omega \in A} 1 \cdot Prob(\{\omega\}) \\ &= Prob(A) \end{aligned}$$

*(ii)* Erwartungswert der Binomialverteilung

$$\begin{aligned} E[X] \overset{\text{Def.}}{=} \textstyle\sum_{k=0}^n k Prob(X = k) &= \textstyle\sum_{k=1}^n k Prob(X = k) \\ &\overset{\text{Bsp. 2.3}}{=} \textstyle\sum_{k=1}^n k \binom{n}{k} p^k (1-p)^{n-k} \\ &= \textstyle\sum_{k=1}^n k \frac{n!}{k!(n-k)!} p^k (1-p)^{n-k} \\ &= \textstyle\sum_{k=1}^n \frac{n(n-1)!}{(k-1)!(n-1-(k-1))!} p p^{k-1} (1-p)^{n-1-(k-1)} \\ &= np \textstyle\sum_{k=1}^n \binom{n-1}{k-1} p^{k-1} (1-p)^{n-1-(k-1)} \\ &\overset{\text{Indexshift}}{=} np \textstyle\sum_{k'=0}^{n'} \binom{n'}{k'} p^{k'} (1-p)^{n'-k'} \\ &= np\, (p + (1-p))^{n'} \\ &= np \end{aligned}$$

## 2.3 Eigenschaften des Erwartungswertes

*Der Erwartungswert hat einige nützliche Eigenschaften, welche das Berechnen stark vereinfachen. Der Erwartungswert der Summe von Zufallsvariablen läßt sich als Summe der Erwartungswerte der einzelnen Zufallsvariablen berechnen. Dies zeigt das*

**2.6 Lemma** *(Linearität des Erwartungswertes)*
*Seien $X, Y$ zwei Zufallsvariablen und $a, b \in \mathbb{R}$. Falls die einzelnen Erwartungswerte existieren, dann gilt:*

$$E[aX + bY] = aE[X] + bE[Y]$$

***Beweis:*** *Seien $T_x, T_y$ die zu $X$ und $Y$ gehörigen Trägermengen.*

$$\begin{aligned}
E[aX+bY] &= \sum_{x\in T_x}\sum_{y\in T_y}(ax+by)P(X=x,Y=y) \\
&= \sum_{x\in T_x}\sum_{y\in T_y} axP(X=x,Y=y) + \sum_{x\in T_x}\sum_{y\in T_y} byP(X=x,Y=y) \\
&\overset{\text{abs. konv.}}{=} \sum_{x\in T_x} ax \underbrace{\sum_{y\in T_y} P(X=x,Y=y)}_{\textit{Randverteilung von } X} + \sum_{y\in T_y} by \underbrace{\sum_{x\in T_x} P(X=x,Y=y)}_{\textit{Randverteilung von } Y} \\
&= a\sum_{x\in T_x} xP(X=x) + b\sum_{y\in T_y} yP(Y=y) \\
&= aE[X] + bE[Y]
\end{aligned}$$

□

Eine weitere wichtige Eigenschaft, die bei allen später behandelten Probleme zum Tragen kommt, ist die

**2.7 Lemma** *(Schubfacheigenschaft)*
*Sei $X$ eine Zufallsvariable und ihr Erwartungswert $E[X]$ existiere. Dann existiert ein $t^* \in \Omega$ mit $X(t^*) \geq E[X]$.*

***Beweis:*** *Angenommen die Aussage gilt nicht, d.h. $\forall t : X(t) < E[X] =: \mu$*

$$\begin{aligned}
E[X] &\overset{\text{Def.}}{=} \sum_{t\in T} P(X=t)\cdot X(t) \\
&\overset{\text{Vor.}}{<} \sum_{t\in T} P(X=t)\cdot \mu \\
&= \mu \cdot \underbrace{\sum_{t\in T} P(X=t)}_{=1} \\
&= \mu \\
&= E[X]
\end{aligned}$$

□

*Dies nennt man die **Schubfacheigenschaft** des Erwartungswertes. Eine analoge Aussage für $X(t^*) \leq E[X]$ für ein $t^*$ ist einfach zu verifizieren.*

Mit dieser Eigenschaft lassen sich alle in nächsten Kapitel behandelten Probleme lösen, da es, wie das Lemma besagt, jeweils eine Realisation eines Zufallsexperimentes mit positiver Wahrscheinlichkeit geben muss, welche größer bzw. kleiner ist als der Erwartungswert aller Experimentrealisationen.

**2.8 Bemerkung** *Im Allgemeinen sind dies keine konstruktiven Beweise, so dass es immer noch ein Problem darstellt, eine konkrete Lösung des Problems anzugeben. Die Schubfacheigenschaft liefert nur den Beweis der Existenz einer Lösung mit den gesuchten Eigenschaften.*

# 3 Anwendungen der Lineartät des Erwartungswertes

Im folgenden werden Beweise aus der jüngeren Vergangenheit gezeigt, die mit Hilfe des stochastischen Ansatzes erst ermöglicht bzw. stark vereinfacht wurden.

## 3.1 Graphentheorie

### 3.1.1 Hamiltonpfade in Turnieren

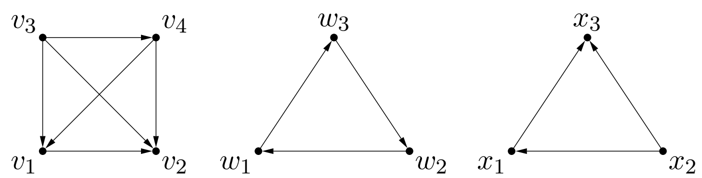
**3.1 Definition** *(Hamiltion-Pfad)*
*Sei $G = (V, E)$ ein Graph. Ein Pfad $H$ heißt **Hamilton-Pfad** genau dann wenn $H$ jeden Knoten $v \in V$ genau einmal enthält.*

Die Definition des Hamilton-Pfades gilt sowohl für gerichtete als auch für ungerichtete Graphen. Diese wird hier aber nur für eine spezielle Unterklasse der gerichteten Graphen, den Turnieren, benötigt.

**3.2 Definition** *(Turniere)*
*Sei ein gerichteter Graph $G = (V, E)$ mit Knotenmenge $V$ und Kantenmenge $E$ gegeben. Wenn für je zwei Knoten $v_1, v_2 \in V$ mit $v_1 \neq v_2$ gilt, dass entweder $(v_1, v_2) \in E$ oder $(v_2, v_1) \in E$, dann heißt $G$ ein **Turnier***

**3.3 Beispiel**

*Turniere*




| | | | |
|---|---|---|---|
| *Hamiltonpfade* | $(v_3, v_4, v_1, v_2)$ | $(w_1, w_3, w_2)$<br>$(w_3, w_2, w_1)$<br>$(w_2, w_1, w_3)$ | $(x_2, x_1, x_3)$ |

**3.4 Satz** (Hamiltion-Pfade in Turnieren [Szele 1943])
Es existiert ein Turnier $T$ mit $n$ Knoten, das mindestens $\frac{n!}{2^{n-1}}$ Hamiltonpfade besitzt.

***Beweis:*** *Nehme ein zufälliges Turnier $T$ mit $n$ Knoten (durch $\frac{n(n-1)}{2}$-fachen Münzwurf). Sei weiterhin $X$ die Zufallsvariable, welche die Anzahl der Hamilton-Pfade angibt. Für jede Permutation der Knotenmenge $\pi = (x_{i_1}, \ldots, x_{i_n}) \in S_n$ sei $\mathbb{1}_\pi^T$ die Zufallsvariable definiert durch*

$$\mathbb{1}_\pi^T = \begin{cases} 1 & , \pi \text{ ist ein Hamilton-Pfad in } T \\ 0 & , sonst \end{cases}$$

*formaler*

$$\mathbb{1}_\pi^T = \begin{cases} 1 & , (x_{i_j}, x_{i_{j+1}}) \in E \ \forall j = 1, \ldots, n-1 \\ 0 & , sonst \end{cases}$$

*Dann läßt sich $X(T)$ darstellen als $X(T) = \sum_{\pi \in S_n} \mathbb{1}_\pi^T$. Mit der Linearität des Erwartungswertes ergibt sich $E[X] = E[\sum_{\pi \in S_n} \mathbb{1}_\pi^T] = \sum_{\pi \in S_n} E[\mathbb{1}_\pi^T]$*
*Der Erwartungswert der Indikatorfunktion $\mathbb{1}_\pi^T$ läßt sich analog zu Beispiel 2.5 berechnen als $E[\mathbb{1}_\pi^T] = Prob('\pi\ ist\ Hamilton - Pfad\,') = \frac{1}{2^{n-1}}$, denn ein Pfad mit $n$ Knoten hat $n-1$ Kanten, welche durch $n-1$ unabhängige Münzwürfe ($p = 0.5$) bestimmt wurden. Alle Ausgänge haben die gleiche Wahrscheinlichkeit, aber nur ein Ausgang beschreibt einen Hamilton-Pfad.*


*Daraus ergibt sich für $E[X] = \sum_{\pi \in S_n} E[\mathbb{1}_\pi^T] = \frac{1}{2^{n-1}} \sum_{\pi \in S_n} 1 = \frac{n!}{2^{n-1}}$*
*Mit Lemma 2.7 folgt die Existenz eines Turniers $T^*$ mit $n$ Knoten, welches mindestens $n!/2^{n-1}$ Hamilton-Pfade besitzt.* □

**3.5 Beispiel**

| *Knoten* | $n$ | 3 | 4 | 5 | 6 | 10 | 20 | 50 |
|---|---|---|---|---|---|---|---|---|
| *#Pfade* | $\frac{n!}{2^{n-1}}$ | 1.5 | 3 | 7.5 | 22.5 | 7087.5 | $4.64 \cdot 10^{12}$ | $5.40 \cdot 10^{49}$ |
| *#Turniere* | $2^{\frac{n(n-1)}{2}}$ | 8 | 64 | 1024 | 32768 | $3.5 \cdot 10^{13}$ | $1.56 \cdot 10^{57}$ | $5.77 \cdot 10^{369}$ |

**3.6 Bemerkung** *(Obergrenze)*
*Es ist weit aus schwieriger, eine maximale Anzahl von Hamilton-Pfade für ein Turnier mit $n$ Knoten zu bestimmen. Daher sei hier nur auf die obere Schranke von $c\sqrt{n^3}\frac{n!}{2^{n-1}}$ für ein $c \in \mathbb{R}^+$ verwiesen.*

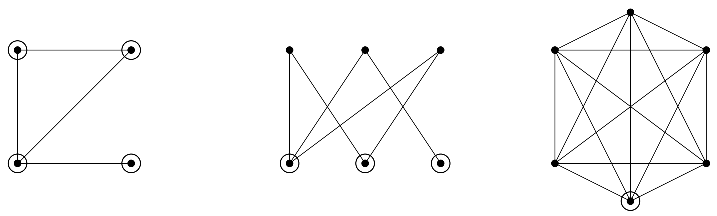
### 3.1.2 Dominierende Mengen

Ein in der Graphentheorie viel untersuchtes Themengebiet ist die Überdeckung von Graphen. Neben dem *Vertex Cover*, bei dem mit einer Auswahl von Knoten die Kanten des Graphen abgedeckt werden, werden auch die dominierenden Mengen betrachtet.

**3.7 Definition** *(Dominierende Mengen)*
*Sei $G = (V, E)$ ein Graph. Weiterhin sei $S \subseteq V$ eine Teilmenge der Knotenmenge. Dann heißt $S$ eine* ***dominierende Menge****, wenn für alle $v \in V$ eine der beiden Bedingungen erfüllt ist.*

$$(i)\ v \in S \quad (ii)\ \exists w \in S\ mit\ \{v, w\} \in E$$

**3.8 Beispiel** *Triviale dominierende Mengen*



ganzer Graph $S = V$ bipartiter Graph vollständiger Graph

Aus den Beispielen ist ersichtlich, dass es keine Schwierigkeit darstellt, eine solche dominierende Menge zu finden, allerdings ist man in der Regel an einer minimalen Teilmenge $S$ interessiert.

**3.9 Satz** *(Größe von dominierenden Mengen [Alon 1990])*
*Sei $G = (V, E)$ ein Graph mit $n = |V|$ Knoten und einem Minimalgrad $d_{min}$. Dann existiert eine dominierende Menge $S$ mit höchstens $|S| = n\frac{1+\ln(d_{min}+1)}{d_{min}+1}$ Knoten.*

***Beweis:*** *Sei $S'$ die Menge, die jeden Knoten $v \in V$ mit der Wahrscheinlichkeit*

$$Prob(v \in S') =: p = \frac{\ln(d_{min}+1)}{d_{min}+1}$$

*enthält. Sei nun weiterhin die Teilmenge $T \subseteq V - S'$ die Menge aller Knoten, die keine Nachbarn in $S'$ haben, d.h. $\forall t \in T : \nexists s \in S'$ mit $\{t, s\} \in E$. Die Vereinigung $S := S'\dot{\cup}T$ ist aufgrund der Konstruktion disjunkt und eine dominierende Menge. Nun gilt es, die erwartete Kardinalität der Menge $S$ abzuschätzen. Mit Hilfe der Linearität des Erwartungswertes und der disjunkten Vereinigung läßt sich $E[|S|]$ berechnen als*

$$E[|S|] = E[|S'\dot{\cup}T|] = E[|S'| + |T|] = E[|S'|] + E[|T|] \tag{1}$$

*Bleibt also die Erwartungswerte für die Menge $S'$ und $T$ zu berechnen. Es gilt analog zu Beispiel 2.5 (Bernoulli-Experiment der Größe n)*

$$E[|S'|] = E[\sum_{v\in V} \mathbb{1}_{S'}(v)] = Prob(S') = np$$

*Da für alle $t \in T$, noch dessen $d_{min}$ Nachbarn, bei der Konstruktion der Menge $S'$ ausgewählt worden, besitzen sie die Wahrscheinlichkeit*

$$Prob(v \in V - S') = 1 - Prob(v \in S') = 1 - p \Rightarrow Prob(t \in T) \leq (1-p)^{d_{min}+1}$$

*Sei $\mathbb{1}_v^T$ die Zufallsvariable definiert durch*

$$\mathbb{1}_v^T = \begin{cases} 1 & , v \in T \\ 0 & , v \notin T \end{cases}$$

*Sie zeigt an ob ein Knoten $v$ zu $T$ gehört oder nicht. Dann ist wegen $(1-p) \leq e^{-p}\ \forall p \in [0, 1]$*

$$E[|T|] = E[\sum_{v\in V} \mathbb{1}_v^T] = \sum_{v\in V} E[\mathbb{1}_v^T] = \sum_{v\in V} Prob(v \in T) \leq n(1-p)^{d_{min}+1} \leq ne^{-p(d_{min}+1)}$$

*Für die erwartete Größe der dominierenden Menge $S$ aus (1) ergibt sich die Abschätzung*

$$\begin{aligned} E[|S|] &= E[|S'|] + E[|T|] \\ &\leq np + ne^{-p(d_{min}+1)} \\ &= n\frac{\ln(d_{min}+1)}{d_{min}+1} + ne^{-\frac{\ln(d_{min}+1)}{d_{min}+1}(d_{min}+1)} \\ &= n\frac{\ln(d_{min}+1)+1}{d_{min}+1} \end{aligned}$$

*Mit der Schubfacheigenschaft folgt die Aussage des Satzes.* □

**3.10 Bemerkung** *(Wahl von p)*
*Warum wählt man $p = \frac{\ln(d_{min}+1)}{d_{min}+1}$? Die Konstruktion der Menge $S$ aus $S'$ und $T$ funktioniert auch mit anderen $p \in (0, 1]$.*
*Aber die Funktion $f(p) := np + ne^{-p(d_{min}+1)}$ nimmt bei diesem $p$ das Minimium an, und man war an einer möglichst kleinen dominierenden Menge interessiert.*

### 3.1.3 Unabhängigkeitszahl

*Auch bei der Unabhängigkeitszahl (engl. independence number) geht es um die Auswahl einer Teilmenge von Knoten, die unabhängig voneinander sind.*

**3.11 Definition** *(Unabhängigkeitszahl)*
*Sei ein Graph $G = (V, E)$ gegeben. Dann ist die Unabhängigkeitszahl $\alpha(G)$ des Graphen definiert als*

$$\alpha(G) := \max_{S \subseteq V} |\{\forall s_1, s_2 \in S : \{s_1, s_2\} \notin E\}|$$

**3.12 Satz** *(Größe von Unabhängigkeitsmengen [Alon,Spencer 1992])*
*Sei $G = (V, E)$ ein Graph mit der Knotenmenge $V = \{v_1, \ldots, v_n\}$ und $d_1, \ldots, d_n$ die assoziierten Knotengrade. Dann gilt*

$$\alpha(G) \geq \sum_{i=1}^{n} \frac{1}{d_i + 1}$$

***Beweis:*** *Wähle gleichverteilt eine Permutation $\pi \in S_n$ mit $Prob(\pi) = 1/n!$. Dann induziert diese eine Ordnung der Knoten $v_{\pi(1)} < v_{\pi(2)} < \ldots < v_{\pi(n)}$. Nun sei $A_i$ das Ereignis, dass alle $d_i$ Nachbarn $v_{j_1}, \ldots, v_{j_{d_i}}$ in dieser Ordnung größer sind als $v_i$.*
*Betrachte für eine beliebige aber feste Permutation die Auswahl von $v_i$ und seinen $d_i$ Nachbarn aus den $n$ Knoten. Es gibt $\binom{n}{d_i+1}$ Möglichkeiten eine $d_i + 1$-elementige Teilmenge auszuwählen.*
*Wenn nun das Ereignis $A_i$ für diese Teilmenge mit geerbter Ordnung gelten soll, so muss das erste Element $v_i$ sein. Dann sind alle $d_i$ Nachbarn nach Definition der Ordnung größer. Aber auf die Reihenfolge der Nachbarn kommt es dabei nicht an, so dass es $d_i!$ Permutationen derer gibt. Analog gibt es $(n - d_i - 1)!$ Möglichkeiten die Nicht-Nachbarn von $v_i$ anzuordnen. Daraus ergibt sich*

$$\begin{aligned} Prob(A_i) &= \tbinom{n}{d_i+1} \tfrac{d_i!(n-d_i-1)!}{n!} \\ &= \tfrac{n! d_i! (n-d_i-1)!}{n!(n-d_i-1)!(d_i+1)!} \\ &= \tfrac{1}{d_i+1} \end{aligned}$$

*Definiere für alle $i = 1, \ldots, n$ die Zufallsvariable*

$$\mathbb{1}_{A_i}^{\pi} = \begin{cases} 1 & , A_i \text{ gilt} \\ 0 & , sonst \end{cases}$$

*Sei nun $U$ die Vereinigung derjenigen $v_i$ für die das Ereignis für das das Ereignis $A_i$ zutrifft. Dann läßt sich die erwartete Größe von $U$ berechnen als*

$$E[|U|] = E[\sum_{i=1}^{n} \mathbb{1}_{A_i}^{\pi}] = \sum_{i=1}^{n} E[\mathbb{1}_{A_i}^{\pi}] = \sum_{i=1}^{n} Prob(A_i) = \sum_{i=1}^{n} \frac{1}{d_i + 1}$$

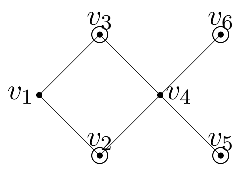
*Mit dem Schubfachprinzip folgt, dass eine Permutation $\pi^*$ existiert mit $|U| \geq \sum_{i=1}^{n} \frac{1}{d_i+1}$. $U$ ist eine unabhängige Menge, denn sei $\{v_i, v_j\} \in E$ eine Kante in $G$, dann gilt*

$$\begin{aligned} v_i < v_j \quad &\Rightarrow \quad v_j \notin U \\ &\textit{oder} \\ v_j < v_i \quad &\Rightarrow \quad v_i \notin U \end{aligned}$$

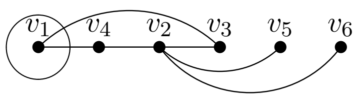
□

**3.13 Beispiel** *(Unabhängigkeitszahl)*

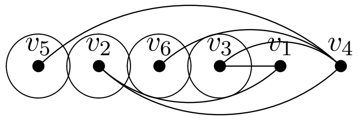
Graph




mögliche Anordnungen




$A_1$ erfüllt




$\alpha(G) = 4 > 2\frac{1}{5} = \sum_{i=1}^{n} \frac{1}{d_i+1}$ $\qquad$ $A_5, A_2, A_6, A_3$ erfüllt

**3.14 Bemerkung** *(Knotengrad)*
*Es ist offensichtlich, dass Knoten mit kleinem Knotengrad in der maximalen Unabhängigkeitmenge bevorzugt werden.*

## 3.2 Kombinatorik

### 3.2.1 Summenfreie Mengen

**3.15 Definition** *(Summenfreie Mengen)*
*Eine Menge $M$ heißt **summenfrei** genau dann, wenn für je zwei Elemente $a, b \in M$ gilt*

$$a \neq b \Rightarrow a + b \notin M$$

**3.16 Satz** *(Summenfreie Teilmenge)*
*Sei $A \subseteq \mathbb{Z} - \{0\}$ mit $|A| = n$. Dann existiert eine Teilmenge $B \subseteq A$ mit $|B| > \frac{n}{3}$.*

***Beweis:*** *Die Idee des Beweises ist die gegebene Menge $A$ auf die bekannte Menge $\mathbb{Z}_p$ mit einer summenfreie Teilmenge abzubilden. Sei $p$ eine Primzahl der Form $p = 3k+2$ mit $p > 2 \cdot \max_{a \in A} |a|$. Konstruiere die Menge $S = \{k+1, \ldots, 2k+1\} = \{k+1, \ldots, k+(k+1)\} \subset \mathbb{Z}_p$. Zu beachten ist, dass $S$ summenfrei ist, denn seien dazu $s_1, s_2 \in S$,*

$$\begin{array}{rcl}
s_1 + s_2 & = & (k+t_1) + (k+t_2) \\
 & = & 2k + t_1 + t_2 \\
\text{mit } t_1 + t_2 & \in & \{2, \ldots, 2k+2\} \\
 & = & \{2, \ldots, k+1\} \,\dot{\cup}\, \{k+2, \ldots, 2k+2\} \\
\Rightarrow s_1 + s_2 & \in & \{2k+2, \ldots, 3k+1\} \,\dot{\cup}\, \{3k+2, \ldots, 4k+2\} \\
 & = & \{2k+2, \ldots, 3k+1\}_{\mathbb{Z}_p} \,\dot{\cup}\, \{0, \ldots, k\}_{\mathbb{Z}_p}
\end{array}$$

*Wähle mit einer Gleichverteilung eine Zahl $t$ aus der Einheitengruppe von $\mathbb{Z}_p$ mit einer Wahrscheinlichkeit $Prob(t) = \frac{1}{p-1}$. Definiere die Abbildung $f_t : A \to \mathbb{Z}_p$ mit $f_t(a) = at \ (mod\ p)$. Definiere weiterhin die Indikatorfunktion für dieses feste $t$ und $\forall\, a \in A, j \in S$*

$$\mathbb{1}_{a,j} = \begin{cases} 1 & , f_t(a) = j \ (mod\ p) \\ 0 & , \text{sonst} \end{cases}$$

*Dann ergibt sich die Anzahl von Elemente aus $A$ die auf die Menge $S$ abgebildet wird als*

$$X := \sum_{a\in A}\sum_{j\in S}\mathbb{1}_{a,j}$$

*Da $\mathbb{Z}_p$ ein Körper im algebraischen Sinne ist, gibt es genau ein $t$ aus $\mathbb{Z}_p - \{0\}$ mit $a \cdot t \equiv_p j$. Daraus ergibt sich*

$$E[\mathbb{1}_{a,j}] = Prob(\mathbb{1}_{a,j} = 1) = Prob(t) = \frac{1}{p-1}$$

*und damit die erwartete Größe von $B$ als*

$$\begin{aligned} E[X] &= E[\textstyle\sum_{a\in A}\sum_{j\in S}\mathbb{1}_{a,j}] \\ &= \textstyle\sum_{a\in A}\sum_{j\in S}E[\mathbb{1}_{a,j}] \\ &= \textstyle\sum_{a\in A}\sum_{j\in S}\frac{1}{p-1} \\ &= \textstyle\sum_{a\in A}\frac{|S|}{p-1} \\ &= \tfrac{n|S|}{p-1} \\ &= \tfrac{nk}{3k-1} \\ &> \tfrac{nk}{3k} = \tfrac{n}{3} \end{aligned}$$

*Wiederum folgt mit dem Schubfachprinzip, dass ein $t^* \in \{1,\ldots,p-1\}$ existiert bei dem die Kardinalität $|B| = |\{a \in A \mid a \cdot t^* = j \ (mod\ p) \text{ mit } j \in S\}| > \frac{n}{3}$.* □

**3.17 Bemerkung** *(Unabhängig von der konkreten Menge)*
*Die ganze Beweiskontruktion ist weitestgehend von der gegebenen Menge $A$ unabhängig. Nur die Wahl der Primzahl hängt von den konkreten Menge ab, was aber nicht ins Ergebnis eingeht.*

**3.18 Beispiel** *(Unabhängige Menge)*
$A = \{1, 2, 3, -1, -2, 5\}, |A| = n = 6$.
*Wähle* $p = 11 = 3 \cdot 3 + 2 > 2\max_{a\in A}|a| \Rightarrow k = 3 \Rightarrow S = \{k+1 = 4, 5, 6, 7 = 2k+1\}$.
*Wähle zufällig* $t = 2$ *und berechne* $\mathbb{1}_{a,j}\ \forall a \in A, j \in S$

| | 1 | 2 | 3 | -1 | -2 | 5 |
|---|---|---|---|---|---|---|
| 4 | 0 | 1 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 1 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 1 | 0 |

$$X = 3 > \frac{6}{3} = 2 \Rightarrow B = \{2, 3, -2\}, |B| = X$$

*Aber diese Auswahl ist nicht maximal, denn die Menge $B' = \{-1, 1, 3, 5\}$ besitzt Mächtigkeit 4.*

**3.19 Bemerkung** *(Maximale Schranke)*
*Alon und Kleitman haben 1990 gezeigt, dass die Verschärfung des Faktors $\frac{1}{3}$ durch $\frac{12}{29}$ beschränkt ist. Die größtmögliche Konstante ist aber zur Zeit nicht bekannt.*

## 3.3 Erfüllbarkeit

**3.20 Definition** *(Literale, Klauseln, Formel)*
*Sei eine Menge $M = \{x_1, \ldots, x_n\}$ von Variablen gegeben. Ein* ***Literal*** *ist dann eine Variable $x_i$ oder ihr Negiertes $\overline{x_i}$. Die Disjunktion (ODER-Verknüpfung) von Literalen über die Menge $M$ nennt man* ***Klausel*** *. Schließlich setzt sich eine (aussagenlogische)* ***Formel*** *als Konjunktion (UND-Verknüpfung) von Klauseln zusammen.*

**3.21 Definition** *(Belegung, Erfüllbarkeit, k-Erfüllbarkeit)*
*Sei eine Formel $F = F(x_1, \ldots, x_n)$ über $n$ Variablen gegeben. Sei weiterhin $b = \{b_1, \ldots, b_n\} \in \{0,1\}^n$ gegeben. Dann ist $b$ eine* ***Belegung*** *von $F$ definiert durch $F(b_1, \ldots, b_n)$.*
*Eine Formel $F$ heißt* ***erfüllbar****, wenn mindestens eine Belegung $b$ existiert, so dass $F(b) = 1$ mit $\bar{0} = 1$ und $\bar{1} = 0$ gilt. Ein etwas schwächere Bedingung ist die* ***k-Erfüllbarkeit****. Sie ist gegeben, wenn mindestens eine Belegung $b$ existiert, so dass für beliebige $k$ Klauseln der Formel $F$, $C_{i_1}, \ldots, C_{i_k}$, diese erfüllt sind.*

### 3.3.1 3-SAT

*Aus der Definition der 3-Erfüllbarkeit folgt, dass eine Belegung existiert, die 3 beliebige Klauseln erfüllt . Der folgende Satz verschärft diese Aussage weiter.*

**3.22 Satz** *(Anzahl erfüllbarer Klauseln [Yannakakis 1994])*
*Sei $F$ eine Formel die 3-erfüllbar ist. Dann existiert eine Belegung $b$ mit der mindestens $\frac{2}{3}$ aller Klauseln gleichzeitig erfüllt werden können.*

***Beweis:*** *Gegeben ist eine 3-erfüllbare Formel $F(x_1, \ldots, x_n)$. Dann konstruiere eine zufällige Belegung $b = (b_1, \ldots, b_n)$ wobei die $b_i$ mit einer Wahrscheinlichkeit*

$$p_{i,1} := Prob(b_i = 1) = \begin{cases} \frac{2}{3} & \text{, F enthällt eine Klausel } x_i \\ \frac{1}{3} & \text{, F enthällt eine Klausel } \overline{x_i} \\ \frac{1}{2} & \text{, sonst} \end{cases}$$

*und folglich*

$$p_{i,0} := Prob(b_i = 0) = \begin{cases} 1 - \frac{2}{3} = \frac{1}{3} & \text{, F enthällt eine Klausel } x_i \\ 1 - \frac{1}{3} = \frac{2}{3} & \text{, F enthällt eine Klausel } \overline{x_i} \\ \frac{1}{2} & \text{, sonst} \end{cases}$$

*Beachte, dass die Klauseln $C_{k_1} = x_i$ und $C_{k_2} = \overline{x_i}$ nicht gleichzeitig in einer 3-erfüllbaren Formel vorkommen können. Somit ist das Wahrscheinlichkeitsmaß wohldefiniert. Zeige zunächst in einem Hilfssatz, dass jedes Klausel $C$ mit einer nach unten beschränkten Wahrscheinlichkeit erfüllt wird.* $\nabla$

**3.23 Lemma** *(Klauselerfüllbarkeit)*
*Sei $b$ eine zufällige Belegung, welche mit obiger Konstruktion ermittelt wurde. Dann wird jede Klausel $C$ mit einer Wahrscheinlichkeit von mindestens $\frac{2}{3}$ erfüllt.*

***Beweis:*** *Beachte dazu, dass jedes Literal $y \in \{x_i, \overline{x_i}\}$ mit einer Wahrscheinlichkeit von maximal $\frac{2}{3}$ nicht erfüllt wird, denn für $y = x_i$ wird mit einer Wahrscheinlichkeit von $p_{i,0}$ und für $y = \overline{x_i}$ mit einer Wahrscheinlichleit von $p_{i,1}$ das Literal nicht erfüllt. Dabei*

*spielt es keine Rolle, ob das Literal als Einheitsklausel oder in Kombination mit anderen Literalen auftritt.*
*Beweise die Aussage für die verschiedenen Klausellängen:*

1. *Einheitsklauseln (Länge 1),*
   *folgt direkt aus der Definition von $p_{i,1}$ bzw. $p_{i,0}$*

2. *Klauseln der Länge $n$, $n \geq 3$,*
   *Jede Einheitsklausel (Literal) wird, wie oben bemerkt, mit einer Wahrscheinlichkeit von höchstens $\frac{2}{3}$ nicht erfüllt. Dann ergibt sich für das Komplementärereignis eine Wahrscheinlickeit von*
   $$\frac{2}{3} = \frac{18}{27} < \frac{19}{27} = 1 - \left(\frac{2}{3}\right)^3 \leq 1 - \left(\frac{2}{3}\right)^n, n \geq 3$$

3. *Klauseln der Länge 2,*
   *Ohne Beschränkung der Allgemeinheit sei $C = (x_1 \vee x_2)$. Unterscheide auch hier zwei Fälle*
   (a) *mindestens ein Literal wird mit einer Wahrscheinlichkeit von $\frac{1}{2}$ erfüllt, das heißt weder das Literal, noch sein Negiertes treten in der Formel als Einheitsklauseln auf. Daraus folgt $C$ wird mit einer Wahrscheinlichkeit von $1 - Prob(b_1 = 0) \cdot Prob(b_2 = 0) \geq 1 - \frac{1}{2} \cdot \frac{2}{3} = \frac{2}{3}$ erfüllt.*
   (b) *beide Literale werden nur mit einer Wahrscheinlichkeit von $\frac{1}{3}$ erfüllt. D.h. die Formel $F$ muss die Klauseln $C' = \overline{x_1}$ und $C'' = \overline{x_2}$ enthalten. Aber die Klauseln $C, C', C''$ können nicht gleichzeitig erfüllt werden, was ein Widerspruch zur 3-Erfüllbarkeit darstellt.*

*Also werden Klauseln beliebiger Länge mit einer Wahrscheinlichkeit von $\frac{2}{3}$ erfüllt.* □

***Beweis:*** *(Fortsetzung von Beweis 3.22)*

*Gegeben ist $F = \bigwedge_{i=1}^{m} C_i$. Definiere die Zufallsvariable $\mathbb{1}_i$ als Indikator für: die i-te Klausel wird von der Belegung $b$ erfüllt.*

$$\mathbb{1}_i = C_i(b)$$

*Dann ergibt sich die Anzahl der erfüllten Klausel in der Formel $F$ unter der Belegung $b$ zu*

$$X := \sum_{i=1}^{m} \mathbb{1}_i$$

*Unter Anwendung der bekannten Eigenschaften des Erwartungswertes läßt sich der Erwartungswert berechnen als*

$$E[X] = E[\sum_{i=1}^{m} \mathbb{1}_i] = \sum_{i=1}^{m} E[\mathbb{1}_i] = \sum_{i=1}^{m} Prob(\mathbb{1}_i = 1) \geq m \cdot \frac{2}{3}$$

*D.h. es existiert eine Belegung $b^*$, so dass mehr als $\frac{2}{3}$ der Klauseln einer Formel erfüllt sind.* □

**3.24 Bemerkung** *(Konstanten für andere $k$)*
*Für die 2-Erfüllbarkeit ergibt sich die Konstante $\frac{2}{1+\sqrt{5}} \approx 0.618$. Man kann zeigen, dass die Konstante für große $k$ gegen $\frac{3}{4}$ konvergiert .*

## 4 Zusammenfassung

*Wir haben in den vergangenen Sätzen und Lemmata gesehen, dass die Wahrscheinlichkeitstheorie, insbesondere des Erwartungswertes und dessen Linearitäts- und der Schubfacheigenschaft, ein mächtiges Werkzeug zum Beweisen ist. Mit ihr lassen sich Beweise kurz und einfach gestalten. Allerdings muss dazu jedes mal das gegebene Problem wahrscheinlichkeitstheoretisch modelliert werden, was oft recht schwierig sein kann und ein Problem für sich darstellt.*
*In den meisten Fällen, wie auch hier, liefern diese Beweise nur die Existenz einer oder mehreren guten Lösungen und nicht deren Konstruktion.*