

Diskrete Strukturen und Logik

WiSe 2006/07 in Trier

Henning Fernau

Universität Trier

fernau@informatik.uni-trier.de

Diskrete Strukturen und Logik

Gesamtübersicht

- Organisatorisches
- Einführung
- Logik & Mengenlehre
- Beweisverfahren
- **Kombinatorik: Die Kunst des Zählens**
- algebraische Strukturen

Varianz und Standardabweichung

Die *Varianz* einer ZV X ist $\text{Var}[X] = E[(X - E[X])^2]$.

Die (positive) Quadratwurzel der Varianz heißt auch *Standardabweichung*.

Da E ein lineares Funktional ist, gilt: $E[X \cdot E[X]] = (E[X])^2$.

→ **Satz:** $\text{Var}[X] = E[X^2] - (E[X])^2$.

Beweis: $\text{Var}[X] = E[(X - E[X])^2] = E[X^2 - 2XE[X] + E[X]^2] = E[X^2] - 2E[XE[X]] + E[X]^2$

Ungleichung von Markoff →

Satz: (Ungleichung von Tschebyscheff) Für $c > 0$ und eine ZV X gilt:

$$P[|X - E[X]| \geq c] \leq \frac{\text{Var}[X]}{c^2}.$$

Varianz Beispiele

Wir betrachten wieder die ZV X_1 und X_{\max} , die mit Würfelexperimenten assoziiert sind.

$\text{Var}[X_1] = E[(X_1 - E[X_1])^2] = E[Y_1]$ für die ZV $Y_1 = (X_1 - 3,5)^2$.

$$E[Y_1] = \sum_{r=(i-3,5)^2, i=1, \dots, 6} r \cdot P[Y_1 = r] = \sum_{r=1, \dots, 6} (r - 3,5)^2 \cdot \frac{1}{6} = \frac{105}{36} \approx 2,92.$$

Alternativer Rechenweg für X_{\max} :

$$\text{Var}[X_{\max}] = E[X_{\max}^2] - E[X_{\max}]^2 = \sum_{r=1, \dots, 6} r^2 P[X_{\max} = r] - \left(\frac{40}{9}\right)^2 = \frac{719}{324} \approx 2,22.$$

Binomialverteilung als ausführliches Beispiel

Erinnerung: $b(k; n, p) = \binom{n}{k} \cdot p^k (1-p)^{n-k}$.

ZV X : Anzahl der “Erfolge” bei “Erfolgswahrscheinlichkeit” p .

$\leadsto P[X = k] = b(k; n, p)$.

$$\begin{aligned} E[X] &= \sum_{k \in [n+1]} k \cdot b(k; n, p) = \sum_{k \in [n+1]} k \cdot \binom{n}{k} \cdot p^k (1-p)^{n-k} \\ &= \sum_{k=1}^n k \cdot \frac{n}{k} \cdot \binom{n-1}{k-1} \cdot p^k (1-p)^{n-k} = n \cdot p \cdot \sum_{k=1}^n \binom{n-1}{k-1} \cdot p^{k-1} (1-p)^{n-k} \\ &= n \cdot p \cdot \sum_{k=0}^{n-1} \binom{n-1}{k} \cdot p^k (1-p)^{n-1-k} = n \cdot p \cdot \sum_{k=0}^{n-1} b(k; n-1, p) = n \cdot p \end{aligned}$$

Binomialverteilung als ausführliches Beispiel (Forts.)

$$\begin{aligned} E[X^2] &= \sum_{k \in [n+1]} k^2 \cdot b(k; n, p) = \dots = n \cdot p \cdot \sum_{k=0}^{n-1} (k+1) \binom{n-1}{k} \cdot p^k (1-p)^{n-1-k} \\ &= n \cdot p \cdot \left(\sum_{k=0}^{n-1} k \cdot b(k; n-1, p) + \sum_{k=0}^{n-1} b(k; n-1, p) \right) = n \cdot p \cdot ((n-1)p + 1) \end{aligned}$$

$$\leadsto \text{Var}[X] = E[X^2] - E[X]^2 = n \cdot p \cdot ((n-1)p + 1) - n^2 p^2 = n \cdot p \cdot (1-p)$$

Zum Umgang mit Summen—ein kombinatorischer Nachtrag

Erster Summationstrick (*geometrische Reihe*):

$$\sum_{k=0}^{\infty} x^k = (1 - x)^{-1} \text{ für } |x| < 1.$$

$$\leadsto \sum_{k=1}^{\infty} x^k = x \sum_{k=1}^{\infty} x^{k-1} = x \sum_{k=0}^{\infty} x^k = x/(1 - x)$$

Zweiter Summationstrick:

Ist $\sum_{k \in \mathbb{N}} f_k(x)$ bekannt, so evtl. auch

(a) $\sum_{k \in \mathbb{N}} f'_k(x)$ und

(b) $\sum_{k \in \mathbb{N}} \int f_k(x)$

durch Vertauschung von Summation und Differentiation oder Integration.

Beispiel:

$$\begin{aligned}\sum_{k=0}^{\infty} k \cdot x^k &= x \cdot \sum_{k=1}^{\infty} k \cdot x^{k-1} = x \sum_{k=1}^{\infty} [x^k]' \\ &= x \cdot \left[\sum_{k=1}^{\infty} x^k \right]' = x \cdot [x/(1-x)]' \\ &= x \frac{(1-x) + x}{(1-x)^2} = \frac{x}{(1-x)^2}\end{aligned}$$

wegen der *Quotientenregel*

$$\left(\frac{u}{v} \right)' = \left(\frac{u'v - v'u}{v^2} \right)$$

Geometrische Verteilung — ein weiteres Beispiel

Wir werfen wiederum wiederholt mit einer Münze, die mit Wahrscheinlichkeit p “Kopf” zeigt. Wie oft muss man werfen, bis das erst Mal “Kopf” erscheint ?

X : ZV, die die Anzahl der nötigen Würfe beschreibt.

Definitionsbereich von X : Menge der endlichen Folgen von Münzwürfen.

$X(e)$ ist dann der Index der ersten Stelle, die “Kopf” ist.

Beispiel: $X((\text{Zahl}, \text{Zahl}, \text{Zahl}, \text{Kopf}, \text{Zahl}, \text{Kopf})) = 4$.

Wertebereich von X : Menge der positiven ganzen Zahlen.

$$P[X = k] = (1 - p)^{k-1}p$$

$P[X = \cdot]$ ist Wahrscheinlichkeitsdichte wegen geometrischer Reihe:

$$\sum_{k=1}^{\infty} P[X = k] = \sum_{k=1}^{\infty} (1 - p)^{k-1}p = p \cdot \frac{1}{1-(1-p)} = 1.$$

$$E[X] = \sum_{k=1}^{\infty} k \cdot (1-p)^{k-1}p = \frac{p}{1-p} \sum_{k=0}^{\infty} k(1-p)^k = \frac{p}{1-p} \cdot \frac{1-p}{p^2} = \frac{1}{p} \text{ gemäß obiger Summationstricks.}$$

Noch ein Beispiel (Fasching ?)

Es werden wiederholt “zufällig” Bonbons an r Kinder verteilt.

Der Versuch eines Kindes, einen geworfenen Bonbon zu fangen, ist ein Bernoulli-Versuch. Jedes der Kinder fängt mit derselben Wahrscheinlichkeit einen Bonbon; die Erfolgswahrscheinlichkeit jedes Kindes ist daher $p = 1/r$.

Wie groß ist die Wahrscheinlichkeit, dass ein bestimmtes Kind von n geworfenen Bonbons genau k fängt ?

Definiere dazu ZV X , deren Wert die Anzahl der von diesem speziellen Kind gefangenen Bonbons beschreibt.

$P[X = k] = b(n; k, 1/r)$, also $E[X] = n/r$.

Wie viele Bonbons müssen geworfen werden, bis dieses spezielle Kind einen Bonbon gefangen hat ?

Definiere dazu ZV Y , die die Nummer des ersten Wurfs angibt, bei dem das Kind ein Bonbon gefangen hat.

$$P[Y = k] = (1 - 1/r)^{k-1} 1/r, \text{ also } E[Y] = r.$$

Wie viele Bonbons müssen geworfen werden, bis jedes Kind einen Bonbon gefangen hat ?

Definiere ZV X_i wie folgt: Wenn bereits $i - 1$ Kinder mindestens einen Bonbon gefangen haben, gebe X_i die Zahl der Würfe an, die noch gemacht werden müssen, bis das i -te Kind einen Bonbon fängt.

Die Misserfolgswahrscheinlichkeit dieses Versuchs ist $(i - 1)/r$.

Alle X_i sind untereinander unabhängig und unterliegen jeweils der geometrischen Verteilung. Also gilt:

$$E[X_i] = \frac{1}{1 - \frac{i-1}{r}} = \frac{r}{r - i + 1}.$$

Für die ZV Z , die angibt, wie viele Versuche unternommen wurden, damit jedes Kind einen Bonbon gefangen hat, gilt: $Z = X_1 + X_2 + \dots + X_r$. Also ist:

$$E[Z] = \sum_{i=1}^r E[X_i] = \sum_{i=1}^r \frac{r}{r-i+1} = r \cdot \sum_{i=1}^r \frac{1}{r}.$$

Wie wir noch sehen werden, ist dies “in etwa gleichbedeutend mit” $r \log_2(r)$ vielen Versuchen.

Die Probabilistische Methode am Beispiel

Erinnerung: Wohlgeformte aussagenlogische Ausdrücke (w.a.A.) bestehen aus Konstanten, Variablen und logischen Verknüpfungen, o.E. Konjunktionen, Disjunktionen und Negationen.

Literale sind nichtnegierte oder negierte Variablen.

k-Disjunktionsterme (auch: *k-Klauseln*) sind Disjunktionen von k Literalen.

Ein w.a.A., der eine Konjunktion von k -Disjunktionstermen ist, liegt in *k-konjunktiver Normalform* vor.

Wie wir später beweisen werden, gilt:

Satz: Zu jedem w.a.A. existiert ein äquivalenter in konjunktiver Normalform.

Die Probabilistische Methode am Beispiel

Ein w.a.A. α heißt *erfüllbar* gdw. es eine Belegung β gibt mit $\beta(\alpha) = w$; β heißt dann auch erfüllende Belegung.

Man kennt keine effizienten, d.h. in Polynomzeit laufenden, Algorithmen, die für gegebenes α dessen Erfüllbarkeit testen können. Dies ist das bekannte *Erfüllbarkeitsproblem* (engl.: satisfiability problem, kurz SAT).

Eine konjunktive Normalform heißt *rein* gdw. für jeden Disjunktionsterm gilt: keine Variable kommt doppelt darin vor.

Mit der so genannten *probabilistischen Methode* kann man jedoch die Erfüllbarkeit gewisser w.a.A. **nicht-konstruktiv** beweisen, ohne deshalb eine erfüllende Belegung zu kennen.

Satz: Jeder w.a.A. in reiner k -konjunktiver Normalform mit $m < 2^k$ Disjunktionstermen ist erfüllbar.

Beweis: Betrachte ein Zufallsexperiment, bei dem jede der Variablen unabhängig voneinander jeweils mit Wahrscheinlichkeit $1/2$ auf “wahr” bzw. “falsch” gesetzt wird (Bernoulli-Experiment).

Betrachte ZV X_i mit $X_i = 1$ falls i -ter Disjunktionsterm nicht erfüllt wird, und $X_i = 0$ sonst. Da der i -te Disjunktionsterm rein ist und k Literale enthält, wird er nur durch eine der 2^k Belegungen seiner Variablen nicht erfüllt.

$\leadsto P[X_i = 1] = 2^{-k} \leadsto E[X_i] = 2^{-k}$. Definiere ZV $X = \sum_{i=1}^m X_i$. Also:

$$E[X] = E\left[\sum_{i=1}^m X_i\right] = \sum_{i=1}^m E[X_i] = mE[X_i] = \frac{m}{2^k} < 1.$$

Wäre nun $P[X = 0] = 0$, so wäre $E[X] = \sum_{i=0}^m i \cdot P[X = i] \geq \sum_{i=1}^m 1 \cdot P[X = i] = 1$, denn $P[X = \cdot]$ ist Wahrscheinlichkeitsdichte. \leadsto **Widerspruch**.

Also ist die Wahrscheinlichkeit, eine erfüllende Belegung durch das Wahrscheinlichkeitsexperiment zu finden, nichtverschwindend. Also existiert so eine Belegung.

Etwas fortgeschrittene Kombinatorik: Doppeltes Abzählen

In der Kombinatorik heißt eine Relation $I \subseteq S \times T$ auch *Inzidenz* und $\iota = (S, T, I)$ heißt *Inzidenzsystem*.

Gilt $(a, b) \in I$, so nennen wir a und b auch (I-)inzident.

Wir führen noch folgende Bezeichnungen ein:

Für $a \in S$ sei $\iota(a)$ die Zahl der mit a inzidenten $b \in T$.

Für $b \in T$ sei $\iota(b)$ die Zahl der mit b inzidenten $a \in S$.

Regel vom Doppelten Abzählen: $\sum_{a \in S} \iota(a) = \sum_{b \in T} \iota(b)$.

Warum gilt die Regel: Veranschaulichung durch *Inzidenzmatrix*

Für $S = \{a_1, \dots, a_m\}$ und $T = \{b_1, \dots, b_n\}$ stelle $m \times n$ -Matrix $M = (m_{ij})$ auf mit

$$m_{ij} = \begin{cases} 1, & \text{falls } a_i I b_j \\ 0, & \text{sonst} \end{cases}$$

$\iota_1(a_i)$: Zahl der Einsen in der i -ten Zeile

$\iota_2(b_j)$: Zahl der Einsen in der j -ten Spalte

Das Handschlaglemma

Ist $G = (V, E)$ ein Graph, so gilt: $\sum_{v \in V} \delta(v) = 2|E|$.

Beweis: Betrachte vIe gdw. $v \in e$ für Inzidenzsystem (V, E, I) .

Folgerung: Jeder Graph hat eine gerade Anzahl von Knoten ungeraden Grades.

Folgerung: Haben alle Knoten in einem Graphen G ungeraden Grad k , so teilt k die Anzahl der Kanten von G .

Teileranzahlen

$t(n)$: Zahl der Teiler der Zahl n

$\bar{t}(n) = \frac{1}{n} \sum_{j=1}^n t(j)$: Durchschnittliche Anzahl der Teiler

Inzidenzsystem: $S = T = \{1, \dots, n\}$ mit $I = |$ (Teilerrelation).

Offenbar gilt: $\iota_2(j) = t(j)$ für $j \leq n$.

Ebenso leicht: $\iota_1(j) = \lfloor \frac{n}{j} \rfloor$.

$$\leadsto \bar{t}(n) = \frac{1}{n} \sum_{j=1}^n \iota_2(j) = \frac{1}{n} \sum_{j=1}^n \iota_1(j) \approx \sum_{j=1}^n \frac{1}{j} \approx \log(n)$$