Das Prinzip des doppelten Abzählens

Es seien X und Y zwei Mengen, welche zueinander in Relation stehen, d.h. es existiert eine Relation $R \subset X \times Y$. Dann gilt

$$\#R = \underbrace{\sum_{x \in X} \#\{y \in Y\colon\ (x,y) \in R\}}_{\text{1. Abzählmöglichkeit}} = \underbrace{\sum_{y \in Y} \#\{x \in X\colon\ (x,y) \in R\}}_{\text{2. Abzählmöglichkeit}} \ .$$

Begründendes Beispiel:

$$X = \{x_1, \ldots\, x_i, \ldots, x_k\}$$
$$Y = \{y_1, \ldots y_j, \ldots, y_\ell\}$$

$$\begin{cases} (x_i, y_j) \in R \iff m_{ij} = 1 \\ (x_i, y_j) \notin R \iff m_{ij} = 0 \end{cases}$$

$$\begin{array}{cc} & \ell = 7 \ \text{Spalten} \\ k = 5 \ \text{Zeilen} & \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix} \end{array}$$

Inzidenzmatrix M einer Relation

i‘te Zeilensumme: $\#\{y \in Y\colon\ (x_i, y) \in R\} = \sum_{1 \le j \le \ell} m_{ij}$

j‘te Spaltensumme: $\#\{x \in X\colon\ (x, y_j) \in R\} = \sum_{1 \le i \le k} m_{ij}$

Beispiel: In einer Vorlesung verteilt der Dozent zu Beginn jeder Sitzung Stifte zum Mitschreiben, die nach jeder Sitzung wieder eingesammelt werden. Jeder Student markiert einen Stift, den er zum ersten Mal benutzt durch einen kleinen Aufkleber mit seinem Namen. Es sei X die Menge der Studenten, Y die Menge der Stifte. Es läßt sich nun folgende Relation definieren: Ein Student x steht in Relation zu einem Stift y, wenn x mindestens einmal y zum Schreiben benutzt hat, d.h. wenn der Stift mit einem Namensaufkleber des Studenten versehen ist.

$$\begin{aligned} \sum_{x \in X} \#\{y \in Y\colon\ (x,y) \in R\} &= \sum_{1 \le i \le k} \#\{y \in Y\colon\ (x_i, y) \in R\} \\ &= \sum_{1 \le i \le k} \sum_{1 \le j \le \ell} m_{ij} \\ &= \sum_{1 \le j \le \ell} \sum_{1 \le i \le k} m_{ij} \\ &= \sum_{1 \le j \le \ell} \#\{x \in Y\colon\ (x, y_j) \in R\} = \sum_{y \in Y} \#\{x \in X\colon\ (x,y) \in R\} \end{aligned}$$

Vertauschen der Summationsreihenfolge

Das Prinzip der doppelten Abzählung resultiert aus der Vertauschbarkeit der Summationsreihenfolge bei endlichen Summen!

Anwendungsbeispiele zu den Abzählregeln

1) Abzählung aller möglichen (x-beliebig.) Abbildungen zwischen endlichen Mengen.
2) Abzählung aller *injektiven* Abbildungen zwischen zwei endlichen Mengen.
   Die Abzählung *surjektiver* Abbildungen ist deutlich komplizierter und erfolgt erst zu einem späteren Zeitpunkt.
3) (anknüpfend an die lineare Algebra, IMI 1) Berechnung der Anzahl von Unterräumen einer vorgegebenen Dimension in einem endlichdimensionalen Vektorraum über einem endlichen Körper. → Anwendung des doppelten Abzählens.
4) Herleitung der Summationsformel für die Quadrate der ersten n natürlichen Zahlen. (**Rückblick:** Aufgabe 1.1 IMI 1 & **Vorausblick:** Integration von Potenzfunktionen)
5) Diskussion des *Geburtstagsparadoxons*.
6) Berechnung der durchschnittlichen Teiler-Anzahl unter den ersten n natürlichen Zahlen. → nochmalige Anwendung des doppelten Abzählens.

Was lehren Beispiel 5 und 6?

Abzählproblem → **Kombinatorik** → Exakte Formel für Abzählung → **Analysis** → handliche Näherungsformel

Definition: Ab- und Aufsteigende Faktorielle

Es sei $x \in \mathbb{C}$ und $n \in \mathbb{N}$.

- n'te *absteigende Faktorielle* von x

$$x^{\underline{n}} := \prod_{k=0}^{n-1} (x-k) = x \cdot (x-1) \cdot \ldots \cdot (x-n+1)$$

- n'te *aufsteigende Faktorielle* von x

$$x^{\overline{n}} := \prod_{k=0}^{n-1} (x+k) = x \cdot (x+1) \cdot \ldots \cdot (x+n-1)$$

- Sinnvolle Konvention: $x^{\underline{0}} := 1 =: x^{\overline{0}}$
- **Fakultät:** $n! := n^{\underline{n}} = n \cdot (n-1) \cdot \ldots \cdot 1$

Sprech- und Schreibweise: Unter einer n-Menge versteht man eine Menge mit n Elementen, d.h. eine n-Menge hat die Mächtigkeit n.

Abzählen von Abbildungen

Satz: Es seien X_n und Y_r zwei endliche Mengen mit $|X_n| = n$ und $|Y_r| = r$. Dann gilt:
1) Es gibt genau r^n Abbildungen von X nach Y, also

$$\#\mathrm{Abb}(X_n, Y_r) \equiv \#\{f: X_n \to Y_r\} = r^n.$$

2) Es gibt genau $r^{\underline{n}}$ *injektive* Abbildungen von X_n nach Y_r, also

$$\#\mathrm{Inj}(X_n, Y_r) \equiv \#\left\{f: X_n \overset{\text{inj.}}{\longrightarrow} Y_r\right\} = r^{\underline{n}}.$$

Beweis: Betrachte als geordnete Mengen: $X_n = \{x_1, \ldots, x_n\}$, $Y_r = \{y_1, \ldots, y_r\}$

Ad 1) $\mathrm{Abb}(X_n, Y_r)$ und $(Y_r)^n$ sind gleichmächtig, denn die Zuordnung

$$f \in \mathrm{Abb}(X_n, Y_r) \quad \mapsto \quad \big(f(x_1), \ldots, f(x_n)\big) \in \underbrace{Y_r \times \ \ldots \ \times Y_r} \ = |Y_r|^n$$

ist *bijektiv*, weil jede Abbildung aus $\mathrm{Abb}(X_n, Y_r)$ auch umgekehrt eindeutig durch ein Tupel aus $(Y_r)^n$ dargestellt wird. *Gleichheitsprinzip* und *Produktregel* liefern daher:

$$\#\mathrm{Abb}(X_n, Y_r) = |Y_r|^n = r^n .$$

$X^n \equiv X \times \ldots \times X \ \leftrightarrow \ \{f: \{1, \ldots, n\} \to X\} \equiv \mathrm{Abb}(\{1, \ldots, n\}, X) \ \wedge \ |X^n| = |X|^n \ \Rightarrow \ \#\mathrm{Abb}(\{1, \ldots, n\}, X) = |X|^n$

Informeller Beweis: Man betrachte n unterschiedliche Kugeln, die in r unterscheidbare Fächer sortiert werden sollen. Durch die Verteilung der Kugeln auf die Fächer entsteht eine Abbildung von der n-Menge der Kugeln in die r-Menge der Fächer. Können die Kugeln irgendwie plaziert werden, so gibt es für jede Kugel r Möglichkeiten insgesamt r^n Möglichkeiten. Darf sich in jedem Fach höchstens eine Kugel befinden, so gibt es für die erste Kugel r Möglichkeiten, für die zweite jedoch nur $r-1$, da bereits ein Fach besetzt ist. Entsprechend bestehen für die zweite Kugel $r-2$ Möglichkeiten usw. bis für die n'te Kugel nur noch $r-n+1$ Möglichkeiten verbleiben. *In toto*, erhält man dann $r \cdot (r-1) \cdot (r-2) \cdot \ldots \cdot (r-n+1) = r^{\underline{n}}$ Möglichkeiten.

Beweis des Satzes

Ad 2) Beweis per *Induktion* über n. **Induktionsanfang** $(n = 1)$ $\#\mathrm{Inj}(X_1, Y_r) = r^{\underline{1}} = r$. ✓

Induktionsschritt:

Klassifikation von $\mathrm{Inj}(X_{n+1}, Y_r)$ nach $f(x_{n+1}) \in Y_r$

$$\mathrm{Inj}(X_{n+1}, Y_r) = \left\{ f : X_{n+1} \xrightarrow{\text{injektiv}} Y_r \right\} = \dot{\bigcup_{1 \le i \le r}} \left\{ f : X_{n+1} \xrightarrow{\text{injektiv}} Y_r \mid f(x_{n+1}) = y_i \right\}$$

Bijektion: $\left\{ f : X_{n+1} \xrightarrow{\text{injektiv}} Y_r \mid f(x_{n+1}) = y_i \right\} \leftrightarrow \mathrm{Inj}\big(X_{n+1} - \{x_{n+1}\},\, Y_r - \{y_i\}\big)$

$$\#\mathrm{Inj}(X_{n+1}, Y_r) = \sum_{1 \le i \le r} \#\left\{ f : X_{n+1} \xrightarrow{\text{injektiv}} Y_r \mid f(x_{n+1}) = y_i \right\}$$

Summenregel

$$= \sum_{1 \le i \le r} \#\mathrm{Inj}\big(\underbrace{X_{n+1} - \{x_{n+1}\}}_{n\text{-Menge}},\, \underbrace{Y_r - \{y_i\}}_{(r-1)\text{-Menge}} \big)$$

Gleichheitsprinzip

Induktionsvoraussetzung

$$= \sum_{1 \le i \le r} (r-1)^{\underline{n}} = (r-1)^{\underline{n}} \sum_{1 \le i \le r} 1$$

$$= (r-1)^{\underline{n}} \cdot r = r^{\underline{n+1}}$$

■

Anwendungsbeispiel aus der Linearen Algebra zum Prinzip doppelten Abzählens

V Verktorraum der Dimension n über dem endlichen Körper K mit $|K| = q$. $\Rightarrow$ $|V| = q^n$.

Gesucht: Anzahl der Unterräume $U \subset V$ mit $\dim U = \ell$?

$X := \{U \subset V\colon \ \dim U = \ell\}$ $\qquad |X| = ?$

$Y := \{(v_1, \dots, v_\ell)\colon \ \dim \operatorname{Span} \ (v_1, \dots, v_\ell) = \ell\}$

Menger aller geordneten ℓ-Tupel linear unabhängiger Vektoren aus V.

Definition der Relation $R \subset X \times Y$:

$$\forall U \in X, \ \forall (v_1, \dots, v_\ell) \in Y\colon \quad \big(U, (v_1, \dots, v_\ell)\big) \in R \quad :\Leftrightarrow \quad U = \operatorname{Span}(v_1, \dots, v_\ell)$$

Prinzip des doppelten Abzählens $\Rightarrow$ Gleichung für $|X|$.

$$\#R = \sum_{x \in X} \#\{y \in Y\colon \ (x,y) \in R\} = \sum_{y \in Y} \#\{x \in X\colon \ (x,y) \in R\}$$

$$\sum_{\substack{U \subset V \\ \dim U = \ell}} \underbrace{\#\left\{\begin{matrix}\text{Menge der} \\ \text{geordneten Basen von } U\end{matrix}\right\}}_{\text{Hängt nur von } \dim U \text{ nicht aber von } U \text{ selbst ab.}} = \sum_{\substack{(v_1,\dots,v_\ell) \subset V \\ \text{lin. unabh.}}} \underbrace{\#\left\{\begin{matrix}\text{Menge der Unterräume} \\ \text{aufgespannt von } (v_1, \dots, v_\ell)\end{matrix}\right\}}_{\text{Die Vektoren spannen genau einen } \ell\text{-dim. Unterraum auf.}}$$

$$\#\left\{\begin{matrix}\text{Menge der geordneten Basen} \\ \text{in einem } \ell\text{−dimen. VR über } K\end{matrix}\right\} \cdot \sum_{\substack{U \subset V \\ \dim U = \ell}} 1 = \sum_{\substack{(v_1,\dots,v_\ell) \subset V \\ \text{lin. unabh.}}} 1$$

Anwendungsbeispiel aus der Linearen Algebra **zum Prinzip doppelten Abzählens**

$$\#\left\{\begin{matrix}\text{Menge der geordneten Basen}\\ \text{in einem } \ell\text{−dimen. VR über } K\end{matrix}\right\} \cdot \sum_{\substack{U\subset V\\ \dim U=\ell}} 1 \;=\; \sum_{\substack{(v_1,\dots,v_\ell)\subset V\\ \text{lin. unabh.}}} 1$$

$$\#\left\{\begin{matrix}\text{Menge der } \ell\text{−Tupel linear unabhängiger}\\ \text{Vektoren in einem } \ell\text{−dimen. VR über } K\end{matrix}\right\} \cdot |X| \;=\; \#\left\{\begin{matrix}\text{Menge der } \ell\text{−Tupel linear unabhängiger}\\ \text{Vektoren in einem } n\text{−dimen. VR über } K\end{matrix}\right\}$$

Allgemeine Frage für $k, m \in \mathbb{N}$ mit $k \leq m$.
Wieviele k-Tupel linear unabhängiger Vektoren können in einem m-dimensionalen Vektorraum W über dem Körper K mit q Elementen ausgewählt werden?

- Auswahl von v_1 : $W \setminus \{0\}$ $\rightarrow$ $q^m - 1 = q^m - q^0$ Möglichkeiten
- Auswahl von v_2 : $W \setminus \mathrm{Span}(v_1)$ $\rightarrow$ $q^m - q$ Möglichkeiten
- Auswahl von v_3 : $W \setminus \mathrm{Span}(v_1, v_2)$ $\rightarrow$ $q^m - q^2$ Möglichkeiten

  $\vdots$ $\vdots$ $\vdots$ $\vdots$
- Auswahl von v_k : $W \setminus \mathrm{Span}(v_1, \dots, v_{k-1})$ $\rightarrow$ $q^m - q^{k-1}$ Möglichkeiten

Alle q^m Vektoren von W außer dem Nullvektor.

Antwort: $(q^m - 1) \cdot (q^m - q) \cdot (q^m - q^2) \cdot \ \dots \ \cdot (q^m - q^{k-1}) = \prod_{i=0}^{k-1} (q^m - q^i)$

Anzahl der Möglichkeiten zur Auswahl von k-linear unabhängigen Vektoren in W.

Also folgt: $(q^\ell - 1) \cdot (q^\ell - q) \cdot \ \dots \ \cdot (q^\ell - q^{\ell-1}) \cdot \ |X| = (q^n - 1) \cdot (q^n - q) \cdot \ \dots \ \cdot (q^n - q^{\ell-1})$

Anzahl ℓ-dimensionalen Unterräume in einem n-dimensionalen VR über K mit $|K| = q$.

$$|X| = N_q(n, \ell) := \frac{(q^n - 1) \cdot (q^n - q) \cdot \ \dots \ \cdot (q^n - q^{\ell-1})}{(q^\ell - 1) \cdot (q^\ell - q) \cdot \ \dots \ \cdot (q^\ell - q^{\ell-1})} \in \mathbb{N}$$

Anwendungsbeispiel aus der Linearen Algebra zum Prinzip doppelten Abzählens

$$N_q(m,k) = \frac{(q^m-1)\cdot(q^m-q)\cdot\ \dots\ \cdot\left(q^m-q^{k-1}\right)}{(q^k-1)\cdot(q^k-q)\cdot\ \dots\ \cdot\left(q^k-q^{k-1}\right)} \in \mathbb{N}$$

Beispiel: $V = \mathbb{F}_2^5$ $\quad \dim V = 5,\quad |V| = 2^5 = 32$

$$N_2(5{,}3) = \frac{(2^5-1)\cdot(2^5-2)\cdot(2^5-2^2)}{(2^3-1)\cdot(2^3-2)\cdot(2^3-2^2)} = \frac{(32-1)\cdot(32-2)\cdot(32-4)}{(8-1)\cdot(8-2)\cdot(8-4)}$$

$$= \frac{31\cdot 30\cdot 28}{7\cdot 6\cdot 4} = 31\cdot 5 = \mathbf{155}$$ Anzahl der 3-dim. Unterräume in $\mathbb{F}_2^5$

Es ergibt sich tatsächlich eine ganze Zahl! Das sieht man dem Ausdruck für $N_q(m,k)$ aufgrund seiner Gestalt als Bruch keineswegs an!

Zum Vergleich: Anzahl der Möglichkeiten drei unterschiedliche vom Nullvektor verschiedene Vektoren in $\mathbb{F}_2^5$ herauszugreifen (ohne Berücksichtigung der Reihenfolge).

$$\binom{32-1}{3} = \frac{31\cdot 30\cdot 29}{3!} = 31\cdot 5\cdot 29 = (30^2-1)\cdot 5 = 899\cdot 5 = 4500-5 = \mathbf{4495}$$

Es gilt allgemein: $N_q(m,k) \ll \binom{q^m-1}{k}$

Es bestehen deutlich mehr Möglichkeiten k vom Nullvektor verschiedene Vektoren herauszugreifen (auch ohne Berücksichtigung der Reihenfolge) als einen k-dimensionalen Unterraum auszuwählen, denn die k Vektoren müssen nicht linear unabhängig sein und spannen daher nicht in jedem Fall einen k-dimensionalen Unterraum auf.

Frage: Wie läßt sich ohne den kombinatorischen Hintergrund bzw. ohne die Interpretationsmöglichkeit zeigen, daß der gebrochene Ausdruck für $N_q(m,k)$ stets ganzzahlig ist?

$$N_q(m,k) = \frac{(q^m-1)\cdot(q^{m-1}-1)\cdot\ \dots\ \cdot\left(q^{m-k+1}-1\right)}{(q^k-1)\cdot(q^{k-1}-1)\cdot\ \dots\ \cdot(q^1-1)} \in \mathbb{N} \quad ?$$

Beachte, es ist hier durch $q^{1+2+\dots+(k-1)}$ gekürzt worden!

$\mathbb{F}_2$ ist Körper zur Restklassenmenge $\mathbb{Z}_2$. Dieser kleinste Körper besteht lediglich aus zwei Elementen, 0 und 1.

Kombinatorische Berechnung von Quadratsummen

Gesucht: $S_2(n) \coloneqq \sum_{k=1}^{n} k^2$

Gesucht ist eine explizite Berechnungsformel, mit welcher sich $S_2(n)$ als Funktion von n direkt berechnen läßt.

Idee: 1) Suche eine Menge $\mathcal{S}_n$ mit $|\mathcal{S}_n| = S_2(n)$.
2) Berechne $|\mathcal{S}_n|$ durch eine geschickte Zerlegung.

Ad 1) $\mathcal{M}_3(\ell) \coloneqq \{(a,b,c) \in \mathbb{N}^3: \quad a,b < c \leq \ell\}$ Es gilt: $|\mathcal{M}_3(n+1)| = S_2(n)$.

$$\mathcal{M}_3(n+1) \coloneqq \biguplus_{k=2}^{n+1} \{(a,b,c) \in \mathbb{N}^3: \quad a,b < c = k\}$$

Zerlegung von $\mathcal{M}_3(n+1)$ durch Klassifikation nach dem Wert der größten Zahl c.

Summenregel & Produktregel

$$\Rightarrow \quad |\mathcal{M}_3(n+1)| \coloneqq \sum_{k=2}^{n+1} (k-1)^2 = \sum_{k=1}^{n} k^2 = S_2(n)$$

Ad 2) $\forall (a,b,c) \in \mathcal{M}_3(n+1) \subset \mathbb{N}^3$:

$$a < b \quad \mathrm{XOR} \quad a = b \quad \mathrm{XOR} \quad b < a.$$

Für $(a,b,c) \in \mathcal{M}_3(n+1) \subset \mathbb{N}^3$ trifft stets genau einer der folgenden drei Fälle zu:

$$\begin{aligned}\Rightarrow \quad \mathcal{M}_3(n+1) = \ & \{(a,b,c) \in \mathbb{N}^3: \ \boldsymbol{a} = \boldsymbol{b} < c \leq n+1\} \\ & \uplus \{(a,b,c) \in \mathbb{N}^3: \ \boldsymbol{a} < \boldsymbol{b} < c \leq n+1\} \\ & \uplus \{(a,b,c) \in \mathbb{N}^3: \ \boldsymbol{b} < \boldsymbol{a} < c \leq n+1\}\end{aligned}$$

Zerlegung von $\mathcal{M}_3(n+1)$ mittels Trichotomiegesetz $a < b, \ a = b, \ b < a$. D.h. die Elemente von $\mathcal{M}_3(n+1)$ werden nach der Anordnungsrelation der ersten beiden Komponenten klassifiziert.