Inklusion & Exklusion

Referenz: Matousek-Nesetřil 2006 Invitation to Discrete Mathematics Section 3.7
Hardy Wright 1975 An Introduction to the Theory of Numbers Chapter 16
Halbeisen-Skript: Kapitel 12

Proposition: Für je zwei Mengen X und Y gilt $|X \cup Y| + |X \cap Y| = |X| + |Y|$.

Bew.: $X' := X \setminus Y$, $Y' := Y \setminus X$, $Z := X \cap Y$

$$\Rightarrow \left.\begin{array}{l} X \cup Y = X' \cup Y' \cup Z \\ X = X' \cup Z \\ Y = Y' \cup Z \end{array}\right\} \text{disjunkt}$$

$$\Rightarrow |X \cup Y| + |X \cap Y| = |X'| + |Y'| + |Z| + |Z| = |X| + |Y|. \qquad \text{qed.}$$

Proposition: Für beliebige Teilmengen $X_1, \ldots, X_n$ einer endlichen Menge X gilt

$$\Big| X \setminus \bigcup_{1 \leqslant i \leqslant n} X_i \Big| = |X| - \sum_{1 \leqslant i \leqslant n} |X_i| + \sum_{1 \leqslant i < j \leqslant n} |X_i \cap X_j| - \ldots + (-1)^n \cdot \big| X_1 \cap \ldots \cap X_n \big|.$$

Genauer gilt

$$\Big| X \setminus \bigcup_{1 \leqslant i \leqslant n} X_i \Big| = \sum_{I \subseteq \{1,\ldots,n\}} (-1)^{|I|} \cdot |X_I|$$

mit

$$X_I := \{ x \in X \mid \forall i \in I : x \in X_i \} = \begin{cases} X & \text{falls } I = \varnothing, \\ \bigcap_{i \in I} X_i & \text{falls } I \neq \varnothing. \end{cases}$$

Beweis:

$$\sum_{I\subseteq\{1..n\}} (-1)^{|I|}\cdot |X_I| = \sum_{I} (-1)^{|I|}\cdot \sum_{x\in X_I} 1 = \sum_{x\in X}\ \sum_{\substack{I\\ x\in X_I}} (-1)^{|I|}$$

Setze $f_i(x) := \begin{cases} 1 & \text{falls } x\in X_i \\ 0 & \text{sonst.} \end{cases}$

$\Rightarrow\ x\in X_I \Leftrightarrow \prod_{i\in I} f_i(x) = 1$

$$= \sum_{x\in X}\ \sum_{I} (-1)^{|I|}\cdot \prod_{i\in I} f_i(x)$$

$$= \sum_{x\in X}\ \sum_{I} \prod_{i\in I} (-f_i(x))$$

$$= \sum_{x\in X}\ \prod_{i=1}^{n} (1-f_i(x))$$

$$(1-f_i(x)) = \begin{cases} 0 & x\in X_i \\ 1 & x\notin X_i \end{cases}$$

$$\prod_{i=1}^{n}(1-f_i(x)) = \begin{cases} 0 & x\in \bigcup_i X_i \\ 1 & \text{sonst.} \end{cases}$$

$$= \left| X \setminus \bigcup_{i=1}^{n} X_i \right| .$$

qed.

Anwendung: Ein Übungsleiter gibt n korrigierte Übungsserien zurück, aber verwechselt sie zufällig. Was ist die Wahrscheinlichkeit, dass alle Teilnehmenden eine falsche Serie erhalten?

$$p_n := \frac{\left|\{\sigma \in S_n \mid \forall i \colon \sigma i \neq i\}\right|}{|S_n|} = \ldots \sum_{k=0}^{n} \frac{(-1)^k}{k!} \longrightarrow \frac{1}{e} \text{ für } n \to \infty.$$

$n!$

Lösung: $X = S_n$

$X_i := \{\sigma \in S_n \mid \sigma i = i\}$

$\Rightarrow X_I = \{\sigma \in S_n \mid \forall i \in I : \sigma i = i\}$

$|X_I| = (n - |I|)!$

$$\Rightarrow \left| X \setminus \bigcup_{i=1}^{n} X_i \right| = \sum_{I \subseteq \{1,..,n\}} (-1)^{|I|} \cdot |X_I| = \sum_{I} (-1)^{|I|} \cdot (n - |I|)!$$

$$= \sum_{k=0}^{n} \binom{n}{k} \cdot (-1)^k \cdot (n-k)! = \sum_{k=0}^{n} \frac{n!}{k!} \cdot (-1)^k$$

$$\Rightarrow p_n = \sum_{k=0}^{n} \frac{(-1)^k}{k!} \longrightarrow \frac{1}{e} \quad \text{für } n \to \infty$$

Allgemeiner: Die Anzahl der Permutationen in S_n mit genau k Fixpunkten ist ...

$$= \sum_{\substack{J \subseteq \{1,..,n\} \\ |J| = k}} \#\{\sigma \in S_n \mid \forall i : i \in J \Leftrightarrow \sigma i = i\} = \binom{n}{k} \cdot \#\{\sigma \in S_n \mid \sigma i = i \Leftrightarrow i \leq k\} = \binom{n}{k} \#\{\sigma \in S_{n-k} \mid \forall i : \sigma i \neq i\}$$

$$\sim \binom{n}{k} \cdot (n-k)! \cdot \frac{1}{e} \sim \frac{n!}{k!} \cdot \frac{1}{e}.$$

Im Folgenden $d \mid n$ immer $d \in \mathbb{Z}^{\geq 1}$.

Möbius-Inversion

In diesem Abschnitt betrachten wir Funktionen $f, g, h, \ldots : \mathbb{Z}^{\geqslant 1} \to \mathbb{C}$.

Definition: Die *Faltung von f und g* ist die Funktion $f * g$ mit

$$(f * g)(n) \;:=\; \sum_{d|n} f\left(\tfrac{n}{d}\right) \cdot g(d). \quad = \sum_{\substack{d,e \geq 1 \\ de = n}} f(e) \cdot g(d).$$

Beispiel: Die Funktion δ mit $\delta(1) = 1$ und $\delta(n) = 0$ für alle $n > 1$.

Grundeigenschaften: Für alle f, g, h gilt

$f * g$	$=$	$g * f$
$(f * g) * h$	$=$	$f * (g * h)$
$\delta * f$	$=$	f

$$(\delta * f)(n) = \sum_{d|n} \underbrace{\delta\left(\tfrac{n}{d}\right)}_{=\begin{cases} 1 & \frac{n}{d} = 1 \\ 0 & \text{sonst.} \end{cases}} \cdot f(d) = f(n)$$

$$[(f*g)*h](n) = \sum_{d|n} (f*g)\left(\tfrac{n}{d}\right) \cdot h(d)$$

$ed = m$

$$= \sum_{e|d|n} f\left(\tfrac{n}{de}\right) \cdot g(e) \cdot h(d) = \sum_{m|n} f\left(\tfrac{n}{m}\right) \cdot \underbrace{\sum_{e \cdot d = m} g(e)\, h(d)}$$

$$= \sum_{m|n} f\left(\tfrac{n}{m}\right) \cdot (g*h)(m) = \big(f*(g*h)\big)(n).$$

qed.

z.B. $\boxed{\tau_0(n) = n^0 = 1}$.

$$(\tau_0 * \tau_k)(n) = \sum_{d|n} \underbrace{\tau_0\left(\tfrac{n}{d}\right)}_{1} \cdot \underbrace{\tau_k(d)}_{d^k}$$

Beispiel: Betrachte die Funktion τ_k mit $\tau_k(n) = n^k$ für $k \in \mathbb{N}$. Dann gilt

$$(\tau_0 * \tau_k)(n) = \sum_{d|n} d^k.$$

Für $k = 0$ ist dies die Anzahl aller Teiler von n, für $k = 1$ die Summe aller Teiler, usw.

Definition: Die *Möbiussche Umkehrfunktion* μ ist definiert durch

$$\mu(n) := \begin{cases} (-1)^k & \text{falls } n \text{ Produkt von } k \text{ paarweise verschiedenen Primzahlen ist,} \\ 0 & \text{sonst.} \end{cases}$$

Satz: Für beliebige f und g gilt:

(a) $\tau_0 * \mu = \delta$.

(b) $\tau_0 * f = g \iff f = \mu * g$.

Beweis: (a) $(\tau_0 * \mu)(n) = \sum_{d|n} \underbrace{\tau_0\left(\tfrac{n}{d}\right)}_{1} \cdot \mu(d) = \sum_{d|n} \mu(d)$.

Sei $n = \prod_{i=1}^{r} p_i^{\nu_i}$ mit p_i prim, paarweise verschieden, $\nu_i \geq 1$.

$d = \prod_{i=1}^{r} p_i^{\mu_i}$ mit $0 \leq \mu_i \leq \nu_i$.

$\mu(d) = \begin{cases} 0 & \text{falls } \exists i: \mu_i \geq 2. \\ (-1)^{\sum \mu_i} & \text{für alle } \mu_i \leq 1. \end{cases}$

$\Rightarrow \sum_{d|n} \mu(d) = \sum_{0 \leq \mu_1, \dots, \mu_r \leq 1} \underbrace{(-1)^{\sum \mu_i}}_{\prod_i (-1)^{\mu_i}} = \prod_{i=1}^{r} \sum_{0 \leq \mu_i \leq 1} (-1)^{\mu_i} = \prod_{i=1}^{r} (1-1) = 0^r = \begin{cases} 1 & r = 0 \\ 0 & \text{sonst,} \end{cases}$

$= \begin{cases} 1 & n = 0 \\ 0 & \text{sonst} \end{cases} = \delta(n)$.

(b): Ist $\tau_0 * f = g$,
so folgt $\mu * g = \mu * (\tau_0 * f) = (\mu * \tau_0) * f = (\tau_0 * \mu) * f \overset{(a)}{=} \delta * f = f$.

Ist $f = \mu * g$,
so folgt $\tau_0 * f = \tau_0 * (\mu * g) = (\tau_0 * \mu) * g = \delta * g = g$.

qed.

$= |\{1 \leq k \leq n \mid \mathrm{ggT}(k,n) = 1\}|.$

Anwendung: Für die *Eulersche φ-Funktion* $\varphi(n) := \left|(\mathbb{Z}/n\mathbb{Z})^\times\right|$ gilt $\varphi = \mu * \tau_1$. Für $n = \prod_{i=1}^r p_i^{\nu_i}$ mit paarweise verschiedenen Primzahlen p_i und Exponenten $\nu_i \geqslant 1$ gilt also

$$\varphi(n) = \prod_{i=1}^r p_i^{\nu_i - 1}(p_i - 1).$$

Beweis: $n = |\{k \in \mathbb{Z} \mid 1 \leq k \leq n\}| = \sum_{d \mid n} |\{k \in \mathbb{Z} \mid 1 \leq k \leq n, \mathrm{ggT}(k,n) = d\}|$

$n = \tau_1(n)$

$k = dm$

$$= \sum_{d \mid n} \underbrace{|\{m \in \mathbb{Z} \mid 1 \leq m \leq \tfrac{n}{d}, \mathrm{ggT}(m, \tfrac{n}{d}) = 1\}|}$$

$$= \sum_{d \mid n} \varphi\left(\frac{n}{d}\right) = (\tau_0 * \varphi)(n).$$

$d = \prod_{i=1}^r p_i^{\mu_i}$

$\Rightarrow \tau_1 = \tau_0 * \varphi$

$\overset{(b)}{\Rightarrow} \varphi = \mu * \tau_1.$

$= \tau_1 * \mu$

$$\varphi\left(\prod_{i=1}^r p_i^{\nu_i}\right) = \sum_{d \mid n} \frac{n}{d} \cdot \mu(d) = \sum_{0 \leq \mu_1, \ldots, \mu_r \leq 1} \prod_{i=1}^r p_i^{\nu_i - \mu_i} \cdot (-1)^{\sum \mu_i}$$

$$= \prod_{i=1}^r \left(p_i^{\nu_i} - p_i^{\nu_i - 1}\right) = \prod_{i=1}^r p_i^{\nu_i - 1} \cdot (p_i - 1).$$

Anwendung: Mit welcher Wahrscheinlichkeit sind zwei zufällige positive ganze Zahlen teilerfremd? Das heisst: Bestimme das asymptotische Verhalten für $N \to \infty$ der Grösse

$$\frac{1}{N^2}\cdot\underbrace{\left|\left\{(m,n)\in\mathbb{Z}^2 \;\middle|\; \begin{array}{c}1\leqslant m,n\leqslant N\\ \mathrm{ggT}(m,n)=1\end{array}\right\}\right|}_{a_N}.$$

Lösung:

$m = n$

$$a_N = 1 + 2\cdot\left|\left\{(m,n)\in\mathbb{Z}^2 \;\middle|\; \begin{array}{c}1\le m<n\le N\\ \mathrm{ggT}(m,n)=1\end{array}\right\}\right|.$$

$$= 1 + 2\cdot\sum_{1\le n\le N}\underbrace{\left|\{1\le m<n,\ \mathrm{ggT}(m,n)=1\}\right|}_{\begin{cases}\varphi(n) & \text{falls } n\ge 2.\\ 0 & \text{falls } n=1.\end{cases}}$$

$$= 1+2\cdot\sum_{2\le n\le N}\varphi(n).$$

$\varphi(1)=1$

$$= -1+2\cdot\sum_{1\le n\le N}\varphi(n)$$

$n = de$

$$= -1+2\cdot\sum_{\substack{d,e\ge 1\\ d\cdot e\le N}}\mu(d)\cdot e$$

$$= -1+2\cdot\sum_{1\le d\le N}\mu(d)\cdot\sum_{1\le e\le\lfloor\frac{N}{d}\rfloor} e$$

$$= -1+2\cdot\sum_{1\le d\le N}\mu(d)\cdot\frac{\left(\lfloor\frac{N}{d}\rfloor+1\right)\lfloor\frac{N}{d}\rfloor}{2}$$

$\frac{N}{d}=\lfloor\frac{N}{d}\rfloor+\vartheta_d$

$0\le\vartheta_d<1.$

$$= -1+\sum_{1\le d\le N}\mu(d)\cdot\left(\frac{N}{d}+1-\vartheta_d\right)\left(\frac{N}{d}-\vartheta_d\right)$$

$$\frac{a_N}{N^2} = \frac{-1}{N^2}+\sum_{1\le d\le N}\mu(d)\cdot\left(\frac{1}{d}+\frac{1-\vartheta_d}{N}\right)\left(\frac{1}{d}-\frac{\vartheta_d}{N}\right)$$

$$= \sum_{1\le d\le N}\frac{\mu(d)}{d^2}+\underbrace{\sum_{1\le d\le N}\frac{\mu(d)}{d}\underbrace{(1-2\vartheta_d)}}\cdot\frac{1}{N}$$

$O\left(\sum_{d=1}^{N}\frac{1}{d}\right)=O(\log N)$

$$+\underbrace{\left(-1+\underbrace{\sum_{1\le d\le N}\mu(d)\cdot\underbrace{(1-\vartheta_d)\vartheta_d}_{|\cdot|\le 1}}_{O(N)}\right)\frac{1}{N^2}}_{O\left(\frac{1}{N}\right)}$$

$$= \sum_{d=1}^{N}\frac{\mu(d)}{d^2}+O\left(\frac{\log N}{N}\right)+O\left(\frac{1}{N^2}\right)$$

$$\xrightarrow{N\to\infty}\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}=\frac{6}{\pi^2}\sim\frac{6}{9.\ldots}\sim\frac{2}{3}.$$

$$\prod_p \left(1-\frac{1}{p^2}\right)^{-1} = \sum \frac{1}{n^2} = \frac{\pi^2}{6} \quad \Rightarrow \quad \prod_p \left(1-\frac{1}{p^2}\right) = \frac{6}{\pi^2}$$

Anwendung: Sei k ein endlicher Körper der Ordnung q. Für jedes $d \geqslant 1$ ist die Anzahl der irreduziblen normierten Polynome vom Grad d in $k[X]$ gleich

$$\boxed{\frac{1}{d} \cdot \sum_{e|d} \mu(\tfrac{d}{e}) \cdot q^e \ > \ 0.}$$

$N := \{f \in k[X] \mid \text{irred. normiert}\}$

$$\prod_{f\in N} (1-X^{\deg(f)})^{-1} = \prod_{f \in N} \sum_{\nu \geq 0} X^{\nu\cdot\deg(f)} = \sum_{\substack{\nu_f \geq 0 \text{ für alle } f\in N \\ \text{fast alle } =0}} \prod_f X^{\nu_f \cdot \deg(f)} = \sum_{\substack{\nu_f\geq 0 \\ \text{fast alle } =0}} X^{\overbrace{\sum_f \nu_f \deg(f)}^{= \deg(\prod_f f^{\nu_f})}}$$

$$= \sum_{\substack{f \in k[X] \\ \text{normiert}}} X^{\deg(f)} = \sum_{d\geq 1} X^d \cdot |\{f \in k[X] \mid f \text{ normiert vom Grad } d\}| = \sum_{d \geq 1} X^d \cdot q^d = \frac{1}{1-qX}.$$

$$\Rightarrow -\log(1-qX) = \log\Big(\prod_{f\in N} \frac{1}{(1-X^{\deg(f)})}\Big) = -\sum_{f\in N} \log(1-X^{\deg(f)})$$

$$X\cdot\frac{d}{dX}\Big| \quad \frac{qX}{1-qX} = \sum_{f\in N} \frac{\deg(f)\cdot X^{\deg(f)}}{1-X^{\deg(f)}}$$

$a_d := \#\{f\in N \mid \deg(f) = d\}$

$$\Rightarrow \frac{qX}{1-qX} = \sum_{d\geq 1} a_d \cdot \frac{dX^d}{1-X^d}$$

$de = n$.

$$\Rightarrow \sum_{n\geq 1} (qX)^n \quad \sum_{d\geq 1} a_d\cdot d\cdot \sum_{e \geq 1} X^{de} = \sum_{n \geq 1}\Big(\sum_{d|n} d\cdot a_d\Big) X^n$$

$$\Rightarrow \boxed{q^n = \sum_{d|n} d a_d} \Rightarrow d a_d = \sum_{e|d} \mu(\tfrac{d}{e})\cdot q^e$$

Folge: Für jede Primpotenz p^n existiert ein endlicher Körper der Ordnung p^n.

$k = \mathbb{F}_p$, $n = d$ $\Rightarrow$ $\frac{1}{d}\cdot \sum_{e|d} \mu(\frac{d}{e}) p^e \geq \frac{1}{d}\Big(p^d - \sum_{1\leq e \leq d/2} p^e\Big) > 0$. $\Rightarrow \exists$ irred. $f \in \mathbb{F}_p[X]$ vom Grad d.

$\mathbb{F}_p[X]/f\cdot\mathbb{F}_p[X]$ = endlicher Körper der Ordnung p^d.