

Kombinatorik

Einführung

Zu beachten:

- Unterscheidbare oder nicht unterscheidbare Objekte
- Mit oder ohne Beachtung der Reihenfolge

Quotienten für die Wahrscheinlichkeit:

$$\frac{\text{günstige Fälle}}{\text{mögliche Fälle}}$$

Probleme beim Bestimmen dieser günstigen und möglichen Fälle:

- Permutationen mit und ohne Wiederholungen
- Auswahlprobleme mit und ohne Wiederholungen

	Permutationen		Ungeordnete Stichprobe	Geordnete Stichprobe
mit Widh	$N = \frac{n!}{p_1! \cdot p_2! \cdot \dots} *$	mit Z.legen	$N = \frac{(s+n-1)!}{s! \cdot (n-1)!} = \binom{s+n-1}{s}$	$N = n^k$
ohne Widh	$N = n!$	ohne Z.legen	$N = \frac{n \cdot (n-1) \cdot \dots \cdot (n-k+1)}{k!} = \binom{n}{k}$	$N = \frac{n!}{(n-k)!} = n \cdot \dots \cdot (n-k+1)$

*: Multinomials-koeffizient: $\binom{n}{n_1, n_2, n_3} = \frac{n!}{n_1! \cdot n_2! \cdot n_3!}$

Unterscheidbare Objekte

$$N = n!$$

Nicht unterscheidbare Objekte

Möglichkeiten aabbac anzuordnen:

$$N = \frac{6!}{3! \cdot 2!}$$

Wobei 3! die möglichen Permutationen der drei “a” und 2! der zwei “b” sind.

Geordnete Stichproben mit Zurücklegen

$$N = n^k$$

Geordnete Stichproben ohne Zurücklegen

$$N = n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot (n-k+1) = \frac{n!}{(n-k)!}$$

Binomische Formel

$$\frac{n!}{k!(n-k)!} = \binom{n}{k}, k = 0 \dots n, 0! = 1$$

$$\binom{n}{k} = \binom{n}{n-k}$$

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1} \iff \binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$$

Binominalkoeffizient

Die Binominalkoeffizienten λ_k in der Entwicklung $(a+b)^n = \sum_{k=0}^n \lambda_k a^{n-k} b^k$ sind:

$$\lambda_k = \binom{n}{k} = \frac{n!}{(n-k)! \cdot k!}$$

TR Eingaben

Berechne: $(a + \frac{1}{a})^4$: expand($(a + \frac{1}{a})^4$)

Berechne: $\binom{10}{2} - \binom{9}{2}$: nCr(10,2) - nCr(9,2)

Berechne: $\binom{x}{2} = 595$: solve(nCr(x,2)=595,x)

Schubfachprinzip: Einfache Form

Falls man n Objekte auf m Mengen verteilt, und n grösser als m ist, dann gibt es mindestens eine Menge, in der mehr als ein Objekt landet.

Schubfachprinzip: Starke Form

Seien q_1, q_2, \dots, q_n natürliche Zahlen. Verteilt man

$$q_1 + q_2 + \dots + q_n - n + 1$$

Objekte auf n Mengen, dann enthält entweder die erste Menge mindestens q_1 Objekte oder die zweite Menge enthält mindestens q_2 Objekte, . . . , oder die n-te Menge enthält mindestens q_n Objekte.

$$\Rightarrow (q_1 - 1) + (q_2 - 1) + \dots + (q_n - 1) = q_1 + q_2 + \dots + q_n - n$$

Hier setzt dann das einfache Schubfachprinzip an.

Induktion

Aufbau:

- Induktionsverankerung - $A(1)$
- Induktionsschluss - $A(n) \rightarrow A(n+1)$

Genauer:

- Induktionsanfang: $A(1)$
- Induktionsschritt:
 - Induktionsbehauptung $A(n+1)$
 - Induktionsvoraussetzung $A(n)$

Gruppen

Gruppenkriterien:		Ordnung einer Gruppe:	$ G $
abgeschlossen	$a \bullet b \in G$	Ordnung eines El. einer Gr.:	$\min(n) : x^n = 1$
assoziativ	$(a \bullet b) \bullet c = a \bullet (b \bullet c)$	Eigenschaften:	$\text{ord}(a) \mid \text{ord}(G), a^{\text{ord}(G)} = 1$
neutrales Element	$a \bullet e = a$		$x^m = 1 \leftrightarrow m = \lambda \cdot n$
inverses Element	$a \bullet \bar{a} = e$		

Untergruppe bestimmen: $\text{ordnung}(x) \rightarrow \text{Gruppieren nach Count} \rightarrow \text{irgendwann} = \text{null} \rightarrow \text{nicht Invertierbar (Tafel überprüfen)}$

Untergruppe der Inv.Elemente: $\text{eulerphiarr}(x) \rightarrow \text{nie} = \text{null} \rightarrow \text{invertierbar (Tafel überprüfen)}$

Wichtig: $Z_x, x = \text{prime} \rightarrow \text{Untergruppe}(1, Z_x)$

Zyklische Gruppen

$G = \langle x \rangle = \{x^0, x^1, x^2, \dots, x^{n-1}\}$	n= Ordnung der Gruppe = Ordnung des Erzeugers
$Z_n : \text{Erzeuger} = a^i \neq e, \text{ für } i < n$	Gruppe mit einer n=Primzahl ist immer zyklisch!

Anzahl Erzeuger: $\text{eulerphimo}(x)$

Erzeuger: $\text{eulerphiarr}(x)$

Ordnung Gruppe: $\text{maltafel}(x)$, Schnittpunkt mit 0 (Schnittpunkt mit 1 = inverses)

Permutationen

$S_x \rightarrow \text{ordnung}(\pi) = \text{anz. Vertauschungen}$

$S_x \rightarrow x! \text{ Elemente} = x! \text{ Vertauschungen}$

$(\pi^{x!} = \pi = \text{id}, \text{ Kriterium für Zyklizität})$

Relationen

Relationen-Kriterien:

reflexiv	$\forall a \in A : (a, a) \in R$
symmetrisch	$\forall a, b \in A : (a, b) \in R \rightarrow (b, a) \in R$
transitiv	$\forall a, b, c \in A : (a, b) \in R \wedge (b, c) \in R \rightarrow (a, c) \in R$

Äquivalenz-Relation

Voraussetzung: Die Relation muss reflexiv, transitiv und symmetrisch sein.

Partition: disjunkte Unterteilung in Untermengen - eine ÄR partitioniert eine Menge in Äquivalenzklassen!

Modulare Arithmetik

- $a \equiv_m b \leftrightarrow a = tm + b \leftrightarrow m|(a - b) \leftrightarrow R_m(a) = R_m(b)$
- $R_m(a + b) = R_m(a) + R_m(b)$
- $R_m(a \circ b) = R_m(a) \circ R_m(b)$
- $a^p \equiv_p a \leftrightarrow a^{p-1} \equiv_p 1$
- $R_p(a^b) = R_p(R_p(a)^{R_{p-1}(b)})$
- $a \in Z_n^* \rightarrow a^{\varphi(n)} \equiv_n 1$

Zahlentheorie

- $a|b \wedge b|c \rightarrow a|c$
- $a|b \wedge b|a \rightarrow a = b = -a$
- $a|b \wedge a|c \rightarrow a|(ub + vc)$
- $a|b \vee a|c \rightarrow a|bc$
- $a|bc \wedge \text{ggT}(a, b) = 1 \rightarrow a|c$

Funktionen

Diophant

$ax + by = n, \text{ggT}(a, b) = d \rightarrow \text{Lösbar falls : } d|n \text{ (diophant(a,b,n))}$
 $x_0, y_0 \rightarrow \text{Erweiterter Euklidischer Algorithmus (extgcd(a,b))}$
 $x = x_0 - t \cdot \frac{b}{\text{ggT}(a,b)}, y = y_0 + t \cdot \frac{a}{\text{ggT}(a,b)}, \text{ in } Z_n \text{ alle Zahlen mod n.}$

Euler PHI

$\varphi(\text{prime}) = \text{prime} - 1$
 $\varphi(x) = |M_x| = \{n \in N | 1 \leq n < x, \text{ggT}(n, x) = 1\}$
 $\varphi(x) = (1 - \frac{1}{p_1})(1 - \frac{1}{p_2})(1 - \frac{1}{p_3})(1 - \frac{1}{p_4})....(1 - \frac{1}{p_x}) \cdot x, p_{1...k} = 1 < p < x, p|x$
 $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n), \text{ggT}(m, n) = 1$
 $\varphi(c) = \varphi(p^d) = p^d - p^{d-1}, p = \text{prime}$