Kombinatorik

Einführung

Zu beachten:

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

Quotienten für die Wahrscheinlichkeit:

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

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	$N = \frac{n!}{p_1! \cdot p_2! \cdot \ldots}$ *	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	$N = \frac{n \cdot (n-1) \cdot (\ldots) \cdot (n-k+1)}{k!} = \binom{n}{k}$	$N = \frac{n!}{(n-k)!} = n \cdot \ldots \cdot (n-k+1)$

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

Unterscheidbare Objekte

$$N = n!$$

Nicht unterscheidbare Objekte

Möglichkeiten aabbac anzuordnen:

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

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

Geordnete Stichproben mit Zurücklegen

$$N = n^k$$

Geordnete Stichproben ohne Zurücklegen

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

Binomische Formel

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

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

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

Binominalkoeffizient

Die Binominalkoeffizienten λ_k in der Entwicklung $(a+b)^n = \sum\limits_{k=0}^{n} \lambda_k a^{n-k} b^k$ 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 $q_1, q_2, ..., q_n$ natürliche Zahlen. Verteilt man

$q_1 + q_2 + ... + q_n - n + 1$

Objekte auf n Mengen, dann enthält entweder die erste Menge mindestens q1 Objekte oder die zweite Menge enthält mindestens q2 Objekte, . . . , oder die n-te Menge enthält mindestens qn Objekte.

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

Hier setzt dann das einfache Schubfachprinzip an.

Induktion

Aufbau:

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

Genauer:

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

Gruppen

Gruppenkriterien:	
abgeschlossen	$a \bullet b \epsilon G$
assoziativ	$(a \bullet b) \bullet c = a \bullet (b \bullet c)$
neutrales Element	$a \bullet e = a$
inverses Element	$a \bullet \bar{a} = e$

Ordnung einer Gruppe:	$\mid G \mid$
Ordnung eines El. einer Gr.:	$min(n) : x^n = 1$
Eigenschaften:	$ord(a) \mid ord(G)$, $a^{ord(G)} = 1$
	$x^m = 1 \leftrightarrow m = \lambda \cdot n$

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

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

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

Produkt von Gruppen

$< G_1 \times G_2, \star >$
$\Rightarrow (a_1...a_n) \star (b_1...b_n) \rightarrow (a_1 \star b_1, a_1....b_n)$
z.B.: $< Z_7, + > \times < Z_5, + >=< Z_{35}, + >$

Untergruppen $H \leq G$

- geschlossen
  - $a \star b \in H$
  - $e \in H$
  - $a^{-1} \in H$

Cosets - Nebenklassen

Sei G = Gruppe und H = Untergruppe, dann sind (rechte) CoSets:
$H \star a = \{h \star a \mid h \in H\} = [a]$
z.B.:
Die Elemente der Gruppe sind $1, 5, 7, 11, 13, 17$ und die Untergruppen:
Untergruppe $a :< 1 >= \{1\}$
Untergruppe $b :< 17 >= \{1, 17\}$
Untergruppe $c :< 7 >=< 13 >= \{1, 7, 13\}$
Untergruppe $d :< 5 >=< 11 >= \{1, 5, 7, 11, 13, 17\}$
Dann sind Nebenklassen:
$[1] = 1 \cdot b = \{1, 17\}$
$[5] = 5 \cdot b = \{5 \cdot 1, 5 \cdot 17\} = \{5, 13\}$
$[7] = 7 \cdot b = \{7, 11\}$
Daraus folgt: $E/b = \{[1], [5], [7]\} = E/b = \{(1), (5), (7)\} = \{(1, 17, 5, 13, 7, 11)\}$
Andere CoSets sind:
$E/a = \{1, 5, 7, 11, 13, 17\} E/b = \{1, 5, 7\} E/c = \{1, 5\} E/d = \{1\}$

Zyklische Gruppen

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

Anzahl Erzeuger: $eulerphimo(x)$

Erzeuger: $eulerphiarr(x)$

Ordnung Gruppe: $maltafel(x)$, Schnittpunkt mit 0 (Schnittpunkt mit 1 = inverses)

Hat eine Gruppe die Ordnung n so ist sie Isomorph zu Z_n

Z_m^*

$a \in Zm, \; dann : \; gcd(a, m) = 1$

$\varphi(m) = Kardinalität(Zm*)$

$a^{\varphi(m)} \equiv_m 1$

$a^{p-1} \equiv_p 1$

$a^{n-1} \equiv_n 1, \; wenn : \; gcd(a, n) = 1$

Permutationen

$S_x \rightarrow ordnung(\pi) = anz. Vertauschungen$
$S_x \rightarrow x! \; Elemente = x! \, Vertauschungen$

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

Relationen

Relationen-Kriterien:

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

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

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

Zahlentheorie

- $a|b \wedge b|c \rightarrow a|c$
- $a|b \wedge b|a \rightarrow a = b = -a$
- $a|b \wedge a|c \rightarrow a|(ub + vc)$
- $a|b \vee a|c \rightarrow a|bc$
- $a|bc \wedge ggt(a,b) = 1 \rightarrow a|c$

Funktionen

Diophant

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

Euler PHI

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

$\varphi(c) = \varphi(p^d) = p^d - p^{d-1},\ p = prime$