Mengenlehre

$\neg(A \vee B) = (\overline{A \vee B})$!

Idempotenz G. $A \vee A = A$, $A \wedge A = A$

De Morgan G. $(\overline{A \vee B}) = \overline{A} \wedge \overline{B}$, $(\overline{A \wedge B}) = \overline{A} \vee \overline{B}$

Identitäts G. $A \vee \emptyset = A$

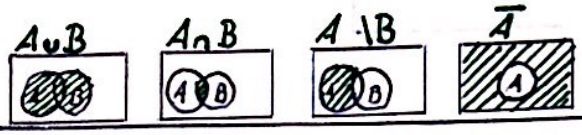
Ω = Universalmenge, $\emptyset$ = leere Menge, $\vee$ = ODER / vereinigt, $\wedge$ = UND / geschnitten

Komplement G. $A \vee \overline{A} = \Omega$, $A \wedge \overline{A} = \emptyset$

Assoziativ G. $(A \vee B) \vee C = A \vee (B \vee C)$, $(A \wedge B) \wedge C = A \wedge (B \wedge C)$

Kommutativ G. $A \vee B = B \vee A$, $A \wedge B = B \wedge A$

Distributiv G. $A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$, $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$



Aussagenlogik

① Negation: $\neg$; $\overline{A}$ ② NAND | ③ NOR ↓ ④ XOR ⊕ ⑤ Konjunktion $\wedge$ (UND) ⑥ Disjunktion $\vee$ (ODER) ⑦ Implikation $A \Rightarrow B$ (folgt) [wwv - vff - fvv - ffv] ⑧ Äquivalenz $\Leftrightarrow$ [www - vff - fvf - ffw]

Umformen

$A \oplus B = (A \wedge \overline{B}) \vee (\overline{A} \wedge B)$

$A \Rightarrow B = \overline{A} \vee B$

$A \Leftrightarrow B = (A \Rightarrow B) \wedge (B \Rightarrow A)$

$A \downarrow B = (\overline{A \vee B})$

$A \mid B = (\overline{A \wedge B})$

Karnaugh: p p $\bar{p}$ $\bar{p}$ / q $\bar{q}$ $\bar{q}$ q

Negationsregeln

$\neg \forall x : p(x) \Leftrightarrow \exists x : \neg p(x)$ | $\forall x \forall y : p(x,y) \Leftrightarrow \forall y \forall x : p(y,x)$

$\neg \exists x : p(x) \Leftrightarrow \forall x : \neg p(x)$ | $\exists x \exists y : p(x,y) \Leftrightarrow \exists y \exists x : p(y,x)$

Zahlensysteme und Restklassen

Exponent bestimmen: $\log_{\text{Rst}}$: log basis Rst

Modulrechnen

55 mod 26 => 55 : 26 = 2, xx => 55 − 2 × 26 = 3

6 mod 7 => 6 : 7 = 0, xx => 6 − 0 × 7 = 6

Kongruenz: $a, b \in \mathbb{Z}$ sind kongruent m wenn $m \in \mathbb{N}$ ein Teiler von $a \equiv b \bmod m$ $a \cdot b$ ist (Bsp: $2 \equiv 16 \bmod 7 \Rightarrow 16 - 2 = 14 : 7 = 2$ R 0)

=> Zahlen aus Restklassen sind kongruent

IEEE / Normalisierte Darstellung

Hin: | 1 bit | 8 bit | 23 bit | = 32 bit

0 = + , 1 = − ; Exp + Bias = 127 ; Exponent > 0 ; Mantisse

S1) Bsp 4,6 => $4 (100)_2$

0,6 = (0,6 − 2^{-1} − 2^{-4} − 2^{-5} − 2^{-8} − 2^{-9} ...)

1 0 0 1 1 0 0 1 1

↳ solange $x - 2^n \geq 0$

info:

$2^{-1} = 0{,}5$

$2^{-2} = 0{,}25$

$2^{-3} = 0{,}125$

$2^{-4} = 0{,}0625$

$2^{-5} = 0{,}03125$

$2^{-6} = 0{,}015625$

S2) 100,1001100$\overline{11}$ Komma verschieben. => 1,xx (1 = hidden bit). Die Stellen um die das "," verschoben ist = Expo hier um 2 nach links => $(\times 00100\overline{11})_2 \cdot 2^2$; rechts wäre 2^{-n} => z.B. bei: 0,0100 2^{-2} => 1 muss vor Komma!

S3) $(4,6)_{10} = (1,00100\overline{11}) \cdot 2^2$ => Exponent = $(2)_{10} + (127)_{10} = (129)_{10} = \underbrace{10000001}_{8\,bit}$ (Bias)

S4) Darstellung: $\underbrace{0}_{V}$ $\underbrace{10000001}_{Exp.\,IE}$ $\underbrace{00100110011001100110011}_{Mantisse\,/\,M}$ B = Bias (127)

Rück:

S1) $x = (-1)^V \cdot 1, M \cdot 2^{(E-B)}$ => 129 − 127 = 2

S2) $x = (-1)^0 \cdot 1, (00100110011001100110011)_2$ (=> jede 1 wird mit 2^{-n} (minus wichtig) dargestellt (23 max)) $\cdot 2^2$

S3) $x = 1, (+2^{-3} + 2^{-6} + 2^{-7} + 2^{-10} + 2^{-11} + 2^{-14} + 2^{-15} + 2^{-18} + 2^{-19} + 2^{-22} + 2^{-23}) \cdot 2^2$

S4) $x = 1$ ((×)14$\overline{5}$) => $1,14\overline{5} \cdot 2^2 = 4,596 \approx 4,6$

Binäre Relationen

① reflexiv, wenn $(a,a) \in R$ für alle $\in A$

② symmetrisch wenn für alle $a, b \in A$ gilt $(a,b) \in R \Rightarrow (b,a) \in R$

③ ant-symmetrisch, wenn für alle $a, b \in A$ gilt: $(a,b) \in R$ und $(b,a) \in R \Rightarrow a = b$ oder $(a \neq b) \Rightarrow (b,a) \notin R$ oder $(a,b) \in R$

④ asymetrisch, wenn für alle $a,b \in A$ gilt: $(a,b) \in R \Rightarrow (b,a) \notin R$

⑤ transitiv, wenn für alle $a,b,c \in A$ gilt: $(a,b) \in R$ und $(b,c) \in R \rightarrow (a,c) \in R$

① 1 2 3 ② 1 2 3 ③ 1 2 3 ④ 1 2 3 ⑤ 1 2 3 (auch 3) Bsp 5: a R b R c

Äquivalenzrelation = reflexiv + transitiv + symmetrisch

Komposition: 2. zuerst => $R_2 \circ R_1$

Summen: $\sum_{i=1}^{n=3} (a_i + b_i) = \sum_{i=1}^{n=3} a_i + \sum_{i=1}^{n=3} b_i = (a_1 + b_1) + (a_2 + b_2) + (a_3 + b_3)$

$\sum_{i=1}^{n=3} (a_i + c) = (a_1 + c) + (a_2 + c) + (a_3 + c)$

Definitionen

$\mathbb{R} = \{-\infty \ldots +\infty\}$ Reelle Zahlen 3,1; 2,5; ...

$\mathbb{Z} = \{-2, -1, 0, 1, 2\}$ Ganzzahlen

$\mathbb{N} = \{1, 2, 3, 4\}$ Natürliche Zahlen

Bsp Mengen

$M_1 = \{x \mid x = 3 \cdot k, k = 0, 1, 2, 3, 4\}$

$M_2 = \{x \mid x \leq 3, x \in \mathbb{Z}\}$

$M_3 = \{x \mid x = 2 \cdot k - 1, k \leq 5, k \in \mathbb{N}\}$

$M_4 = \{x \mid x = 2 \cdot k, k \leq 5, k \in \mathbb{N}\}$

Generated by CamScanner

Modulare Inverse (Cäsar) ggT(11,26)

I $11 = 0 \cdot 26 + 11$ für 4 einsetzen — noch 4 umstellen: $-2 \cdot 11 + 26 = 4$

$26 = 2 \cdot 11 + 4$

$11 = 2 \cdot 4 + 3$ für 3 einsetzen — noch 3 umstellen: $11 - 2 \cdot 4 = 3 \Rightarrow -2 \cdot 4 + 11 = 3$

$4 = 1 \cdot 3 + 1$ (nach 1 umgestellt)

$3 = 3 \cdot 1 + 0$

II $1 = -1 \cdot (3) + 4$

$1 = -1 \cdot (-2 \cdot 4 + 11) + 4$

$1 = 2 \cdot (4) - 11 + (4)$

$1 = 2 \cdot (-2 \cdot 11 + 26) - 11 + (-2 \cdot 11 + 26)$

$1 = -4 \cdot 11 + 2 \cdot 26 - 11 + (-2 \cdot 11) + 26$ || $-2 \cdot 11 + -4 \cdot 11 = -6 \cdot 11$ || $2 \cdot 26 + 26 = 3 \cdot 26$

$1 = -6 \cdot 11 + 3 \cdot 26 - 11$ || $-6 \cdot 11 - 11 = -7 \cdot 11$

$1 = -7 \cdot 11 + 3 \cdot 26 \mod 26$

$1 = -7 \cdot 11 \mod 26 + 3 \cdot 26 \mod 26$ (3·26 mod 26 entfällt = 0)

$1 = -7 \cdot 11 \mod 26 \Rightarrow -7 + 26 = 19$

t	3	5	7	9	11	15	17	19	21	23	25
9	21	15	3	19	7	23	11	5	17	25	

mod. Inv. m 26

Immer versuchen Mod-Werte und Schlüssel zu kürzen bevor ausrechnen: hier 11, 26 (nicht ausrechnen)

Achtung beim Ausmultiplizieren! $2 \cdot (-2 \cdot 11) \Rightarrow -4 \cdot 11$!!! $(2 \cdot -2 \cdot 11)$

Cäsarverschlüsselung mittels modularer Inverse

S = Schlüssel (Verschiebung) Bsp S = 6

t = Faktor (muss mod. Inverse zum Modul haben) Bsp t = 3

m = Modul (i.d.R. 26) m = 26

⇒ untersuchen, ob t modulare Inverse hat; t modul 26 ggT(3,26) = 9

Verschlüsseln

① Wort in Zahlen (0–25)

② Zahlen um Schlüssel verschieben ⇒ Zahl + s mod 26 ⇒ 7 + 6 mod 26 = 13

③ Vert aus ② x t mod 26 ⇒ 13 × 3 mod 26 = 13

Entschlüsseln

① Wort in Zahlen (0–25)

② Zahlen x mod. Inv. mod 26 ⇒ 9 × 13 mod 26 = 13 (9 = mod. Inv. von 3; Buchst. verschoben 13 = Buchstabe entschlüsselt Stufe I)

③ Verschiebung aufheben; Vert aus ② − s mod 26: 13 − 6 mod 26 = 7

Kombinatorik	Variation mit Reihenf.	Kombination ohne Reihenfolge	Permutation alle Elemente
mit Wdh. mit zurücklegen	n^m	$\frac{(n+m-1)!}{m! \cdot (n-1)!}$ $\binom{n+m-1}{m}$	Möglichkeiten! / Gleiche Elemente! $= \frac{3!}{2!}$
ohne Wiederholung ohne zurücklegen	$\frac{n!}{(n-m)!}$	$\frac{n!}{m! \cdot (n-m)!}$ $\binom{n}{m}$	$n!$

m = Auswahl (klein) n = alle Objekte (groß Auswahlmenge)

UND = Multiplikation ODER = Addition

Reihenfolge nicht 7x beachten Bsp: Passwort mit 2 Buchstaben + 4 Zahlen

6 Zeichen PW besteht aus 2 Buchst. + 4 Ziffern; Ziffern wiederholbar, Buchstaben nicht

$2 \times 26 = 52$ ⇒ 2 Ziehen m.R., o.W.

$\frac{52!}{(52-2)!} = 2625$ 2 Buchst. auf 6 Felder verteilt ⇒ 7 V. o R. (schon berücksichtigt)

$\binom{6}{2} = 15 \mid 10^4$ Ziffern m.V. m R.

$\Rightarrow (2625 \times 15) \times 10^4$

Lieferung von 10 enthält 3 fehlerh. Eine Stichprobe von 5 wird genommen. Wie viele Proben o.R. o.V. $\binom{10}{5} = 252$ Wie viele Proben mit 2 defekten?

det det ok

2 aus 3 oR o V $\binom{3}{2} \times \binom{7}{3}$

6 Gäste und 1 Kerl = 7 Schütteln Hand ⇒ also 2 ausgewählt. o.R. o.V. $\binom{7}{2}$

PW aus drei bis fünf Zeichen m.R. m.V. 26^3 oder 26^4 oder 26^5

Club = 12 Mitglieder Wie viel Mögl. 1 sprecher 1 Kaiser 1 Kassenwart? $= 12 \cdot 11 \cdot 10$ für jede Stelle gibt es noch die genannten Auswahlmöglichk.

Pers. a,b,c,d sollen vortragen Wie viele Reihenfolgen sind möglich? ⇒ 4!

Wenn a zuerst sprechen soll = 3!

d nicht zuletzt sprechen soll? 4! − 3!

Wie viele 5stellige Dualzahlen beginnen mit 11 oder enden mit 00.

m R. m.W. $2^3 + 2^3 - 2^1$

11000 00011 11x11 11x11

$P_r(L) = 0,4$ $P_r(K) = 0,5$ $P_r(K \cap L) = 0,4$ L = gelernt K = bestanden

$P_r(K|L) = \frac{P_r(K \cap L)}{P_r(L)} = \frac{0,4}{0,4} = 1$ ⇒ wer gelernt hat, besteht!

① bedingte Wahrscheinlichkeit $P_r(B|A) = \frac{P_r(A \cap B)}{P_r(A)}$, $P_r(A|B) = \frac{P_r(A \cap B)}{P_r(B)}$

② verwenden der Definition $P_r(B|A) = \frac{P_r(A|B) \cdot P_r(B)}{P_r(A)}$

③ $P_r(A)$ durch Satz der totalen W. ersetzen $P_r(B|A) = \frac{P_r(A|B) \cdot P_r(B)}{P_r(A|B) \cdot P_r(B) + P_r(A|\bar{B}) \cdot P_r(\bar{B})}$

$P_r(K|\bar{L}) = \frac{P_r(\bar{L}|K) \cdot P_r(K)}{P_r(\bar{L})} = \frac{0,2 \cdot 0,5}{0,6} = 0,166$ ($P_r(\bar{L}|K)$: 0,5; $P_r(\bar{L})$: 1 − 0,4)

$P_r(\bar{L}|K) = 1 - (P_r(L|K)) = 1 - \frac{0,4}{0,5} = 0,2$

$P_r(L|K) = \frac{P_r(L \cap K)}{0,5} = \frac{0,4}{0,5}$

Generated by CamScanner