Diskrete Mathematik

Woche 6

Shivram Sambhus (cs.shivi.io)

ETH Zurich

Heutige Agenda

1. **Admin & Fragen zu Relationen**
2. **Hauptthema 1: Funktionen**
   - Definitionen & Eigenschaften
   - Komposition & Inverse
3. **Hauptthema 2: Abzählbarkeit**
   - Definitionen & Theoreme
   - Diagonalargument
4. **Hauptthema 3: Kardinalität**
   - Äquivalente Mengen
   - Abzählbar vs. überabzählbar
5. **Übungsteil: Funktionen & Abzählbarkeit**
6. **Vorschau & Tipps**

Admin & Relationen

- **Korrekturen:** Die Korrekturen für Serie 5 sind draussen!
- **Typischer Fehler in der letzten Serie:**
  - **Problem:** Bei Beweisen mit Quantoren: "$\forall x \in A$ (...)" ist nicht gültig. Verwende stattdessen "Sei $U = A$, $\forall x \in U$ (...)" oder starte mit "Für beliebige $a, b \in A$, ...".
  - **Warum?** In der Mengenlehre definieren wir Universen explizit.
  - **Beispiel:** Statt "$\forall x \in A : x \in A$" schreibe "Sei $U = A$, $\forall x \in U : x \in A$".
- **Fragen zu Relationen?**

Hauptthema 1: Funktionen - Theorie

Was ist eine Funktion?

- **Definition:** Eine Funktion $f : A \to B$ ist eine spezielle Relation von A (Domain/Definitionsbereich) nach B (Codomain/Zielbereich). Sie ist total (jedes $a \in A$ wird abgebildet) und well-defined (jedes $a \in A$ hat genau ein $b \in B$ mit $f(a) = b$).
- **Formale Definition:** $f : A \to B$ mit $\forall a \in A \exists b \in B : (a, b) \in f$.
- **Intuitive Notation:** $a \mapsto f(a)$.
- **Beispiel:** Die Quadratfunktion $f : \mathbb{N} \to \mathbb{N}$, $n \mapsto n^2$. Jedes n wird auf genau ein Quadrat abgebildet.

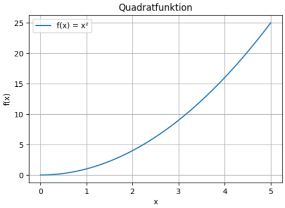


Figure 1: Quadratfunktion

Sanity Check: Häufige Fehler bei Funktionen

- **Well-defined?** Ist $f(a)$ eindeutig für jedes $a \in A$? Z.B. $f : \mathbb{N} \to \mathbb{N}$, $n \mapsto n/2$ wenn n gerade, sonst undefiniert – nicht eindeutig für ungerade n.
- **Total?** Wird jedes $a \in A$ abgebildet? Z.B. $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto 1/x$ ist nicht total bei $x = 0$.
- **Inverse als Relation:** Die "Inverse" von $f(x) = x^2$ ist eine Relation (nicht Funktion), da $\sqrt{x}$ zwei Werte hat ($+\sqrt{x}$ und $-\sqrt{x}$). Funktionen brauchen genau einen Output.
- **Domain/Codomain:** Achte auf A und B. Z.B. $f : \mathbb{Z} \to \mathbb{N}$, $x \mapsto |x|$ ist total, aber Codomain muss passen.
- **Notation:** $f(a) = b$ bedeutet $(a, b) \in f$.

Tipp: Immer prüfe: Totalität und Well-Definiertheit zuerst!

Beispiele: Funktion oder Nicht?

- **Funktion (Total und Well-Defined):** $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x + 1$. Warum: Jeder Input hat genau einen Output.
- **Nicht Funktion (Nicht Total):** $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto \frac{1}{x}$. Warum: Nicht definiert bei $x = 0$.
- **Nicht Funktion (Nicht Well-Defined):** $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto \sqrt{x^2}$. Warum: Mehrdeutig (kann x oder $-x$ sein).

Funktionen vs. Relationen

- **Relation:** Eine Teilmenge $\rho \subseteq A \times B$. Kann mehrere Outputs pro Input haben (z.B. "ist älter als").
- **Funktion:** Spezielle Relation, bei der jeder Input genau einen Output hat. Keine Mehrdeutigkeit.

Bild (Image) und Urbild (Preimage)

- **Bild (Image):** Für $A' \subseteq A$, $f(A') = \{b \in B \mid \exists a \in A' \; f(a) = b\}$. Wir können Mengen in Funktionen einsetzen.
- **Urbild (Preimage):** Für $B' \subseteq B$, $f^{-1}(B') = \{a \in A \mid f(a) \in B'\}$. Immer definiert, auch wenn f^{-1} nicht existiert.
- **Beispiel:** $f : \mathbb{N} \to \mathbb{N}$, $n \mapsto n^2$. Bild von $\{1, 2\} = \{1, 4\}$, Urbild von $\{4\} = \{2\}$.

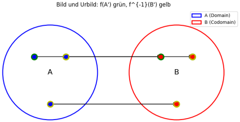


Figure 2: Bild und Urbild Diagramm

Eigenschaften von Funktionen

- **Injektiv (injective):** Verschiedene Inputs $\to$ verschiedene Outputs. $\forall a \forall a' [a \neq a' \to f(a) \neq f(a')]$ (äquivalent zu $\forall a_1, a_2 \in A : f(a_1) = f(a_2) \implies a_1 = a_2$).
  - **Wichtig:** Nicht $a_1 = a_2 \implies f(a_1) = f(a_2)$ (das gilt immer für Funktionen, da well-defined). Die richtige Richtung verhindert, dass verschiedene Inputs zum gleichen Output führen.
  - **Für endliche Mengen:** Äquivalent zu $|A| = |f(A)|$.
- **Surjektiv (surjective):** Jedes Output wird erreicht. $\forall b \in B \exists a \in A : f(a) = b$, oder äquivalent $f(A) = B$.
- **Bijektiv (bijective):** Injektiv und surjektiv. Hat Inverse $f^{-1} : B \to A$.

Prüfung von Funktionseigenschaften

Prozedur für Injektivität:

1. Annahme: Es gibt $a_1, a_2 \in A$ mit $a_1 \neq a_2$ und $f(a_1) = f(a_2)$.
2. Zeige, dass dies unmöglich ist: Aus $f(a_1) = f(a_2)$ folgt $a_1 = a_2$ (via Funktionsdefinition oder Algebra).
3. Schluss: Keine solchen a_1, a_2 existieren, also injektiv.

Beispiel: $f : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto 2x$.

- Annahme: $a \neq b$, $2a = 2b$.
- Dann $a = b$ (dividiere beide Seiten durch 2).
- Also injektiv.

Prozedur für Surjektivität:

1. Für jedes $b \in B$, finde ein $a \in A$ mit $f(a) = b$.
2. Zeige, dass dies immer möglich ist.

Beispiel: $f : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto 2x$.

- Für gerades $b = 2k$, nimm $a = k$.
- Für ungerades b, kein a (da $2a$ immer gerade).
- Also nicht surjektiv.

Komposition von Funktionen

- **Definition:** $(g \circ f)(a) = g(f(a))$.
- **Eigenschaften:** Assoziativ ($(h \circ g) \circ f = h \circ (g \circ f)$), aber nicht kommutativ ($g \circ f \neq f \circ g$ im Allgemeinen).
- **Identität:** $id_A \circ f = f = f \circ id_A$.
- **Inverse:** Nur bijektive Funktionen haben Inverse. $(f^{-1} \circ f)(a) = a$, $(f \circ f^{-1})(b) = b$.

Beispiel: $f : x \mapsto x + 1$, $g : x \mapsto x^2$. Dann $g \circ f : x \mapsto (x + 1)^2$.

Schnell-Check: Funktionseigenschaften

- Ist $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^3$ injektiv? Surjektiv? Bijektiv?
- Was ist das Bild von $\{0, 1, 2\}$ unter $f : \mathbb{N} \to \mathbb{N}$, $n \mapsto n \mod 3$?

Inverse Funktion

- **Bedingung:** f muss bijektiv sein.
- **Eigenschaft:** $(f^{-1} \circ f) = id_A$, $(f \circ f^{-1}) = id_B$.

Übungen zu Funktionen

Übung 1: Ist $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ injektiv? Surjektiv? Bijektiv?
Übung 2: Berechne $(f \circ g)(2)$ für $f(x) = x + 1$, $g(x) = 2x$.
Übung 3: Hat $f : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto x + 1$ eine Inverse? Warum?

Lösungen zu Übungen

Übung 1: Injektiv: Nein (z.B. 2 und -2). Surjektiv: Nein (negative Werte). Bijektiv: Nein.
Übung 2: $g(2) = 4$, $f(4) = 5$.
Übung 3: Ja, bijektiv. Inverse: $x \mapsto x - 1$.

Hauptthema 2: Abzählbarkeit und Kardinalität

Einführung: Verschiedene Unendlichkeiten

Es gibt verschiedene Arten von Unendlichkeit. Die natürlichen Zahlen $\mathbb{N}$ sind unendlich, aber vielleicht gibt es 'grössere' Unendlichkeiten? Heute lernen wir, warum einige Mengen aufzählbar sind (wie eine endlose Liste) und andere nicht—and warum das wichtig ist.

Intuition: Endlich vs. Unendlich

- **Endlich:** Kann zu einem Ende gezählt werden (z.B. 1,2,3,...,100).
- **Unendlich:** Kein Ende (z.B. $\mathbb{N}$: 1,2,3,...).

Intuition: Aufzählbar vs. Nicht-Aufzählbar

- **Aufzählbar (countable):** Kann wie $\mathbb{N}$ nummeriert werden (1: erstes Element, 2: zweites, etc.).
- **Nicht-Aufzählbar (uncountable):** Zu 'gross', keine solche Liste möglich.
- **Beispiel:** Die ganzen Zahlen $\mathbb{Z}$ sind aufzählbar: 0,1,-1,2,-2,... Die reellen Zahlen $\mathbb{R}$? Viel grösser—keine Liste passt!

Definitionen

- **Äquivalent (equinumerous):** $A \sim B$ falls es eine Bijektion $A \to B$ gibt. (Zwei Mengen haben die gleiche 'Grösse'.)
- **Dominiert (dominates):** $A \preccurlyeq B$ falls es eine Injektion $A \to B$ gibt. (Eine Menge 'passt' in eine andere ohne Überschneidungen.)
- **Abzählbar (countable):** $A \preccurlyeq \mathbb{N}$. Entweder endlich oder $\sim \mathbb{N}$. (Hat die 'Grösse' von $\mathbb{N}$—aufzählbar.)
- $\{0,1\}^{\mathbb{N}}$ **(oder** $\{0,1\}^{\infty}$**):** Die Menge der unendlichen Binärfolgen, äquivalent zu Funktionen $\mathbb{N} \to \{0,1\}$. (Z.B. 010101…)

Beispiele: Endliche und Unendliche Mengen

- **Endlich:** $\{1, 2, 3\}$ (5 Elemente).
- **Unendlich:** $\mathbb{N}$ (kein Ende).
- **Vergleiche:** Gerade Zahlen $\sim$ Ungerade Zahlen (beide $\sim \mathbb{N}$).
- **Ungerade vs. Primzahlen:** Ungerade $\sim \mathbb{N}$, Primzahlen $\sim \mathbb{N}$ (beide countable).
- $\mathbb{N}$ **vs. Primzahlen:** Beide countable, aber $\mathbb{N} \sim$ Primzahlen? Nein, aber beide $\preccurlyeq \mathbb{N}$.

Sanity Check: Sind die geraden Zahlen endlich oder unendlich? Countable?

Wichtige Abzählbare Mengen: $\mathbb{N} \times \mathbb{N}$

- **Theorem:** $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$ (Cantor's Pairing: $(a, b) \mapsto \frac{(a+b)(a+b+1)}{2} + b$).
- **Intuition:** Paare (a,b) können wie eine endlose Tabelle nummeriert werden.

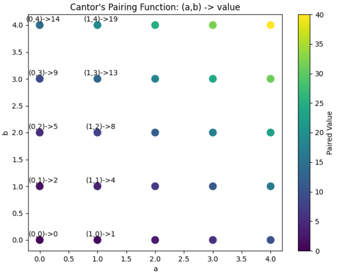


Figure 3: Cantor's Pairing Function

Wichtige Abzählbare Mengen: $\{0,1\}^*$

- **Theorem:** $\{0,1\}^* \sim \mathbb{N}$ (Endliche Binärstrings).
- **Intuition:** Jede endliche Folge kann als Zahl interpretiert werden.

Wichtige Abzählbare Mengen: $\mathbb{Q}$

- **Theorem:** $\mathbb{Q} \sim \mathbb{N}$ (Rationale Zahlen via Paarung).
- **Intuition:** Rationals können in einem Gitter angeordnet und nummeriert werden.

Prozedur: Abzählbarkeit Beweisen

Prozedur: Um zu zeigen, dass A abzählbar ist:

1. Finde eine Injektion $f : A \to \mathbb{N}$ (dann $A \preccurlyeq \mathbb{N}$).
2. Oder konstruiere eine Bijektion $g : \mathbb{N} \to A$ (dann $A \sim \mathbb{N}$).

Tricks:

- **Fundamental Theorem of Arithmetic (FTA):** Verwende Primfaktorzerlegung für Injektionen, z.B. $f(a, b) = 2^a 3^b$.

Cantor-Bernstein Theorem

- **Theorem:** Wenn $A \preccurlyeq B$ und $B \preccurlyeq A$, dann $A \sim B$.
- **Intuition:** Wenn zwei Mengen sich gegenseitig "injizieren" lassen, haben sie die gleiche Grösse.
- **Einfach:** Injection hin und zurück bedeutet Bijection.

Überabzählbarkeit

- **Theorem:** $\{0,1\}^\infty$ ist überabzählbar (Diagonalargument).
- **Intuition:** Stell dir vor, du listest alle unendlichen Binärfolgen. Wir zeigen, warum immer eine fehlt.
- **Beweis (Diagonalargument):**
  - Annahme: Es gibt Bijektion $f : \mathbb{N} \to \{0,1\}^\infty$.
  - Konstruiere α als Komplement der Diagonale: $\alpha_n = 1 - f(n)_n$.
  - α ist in der Menge, aber nicht im Bild von f. Widerspruch.

Computability

- **Definition:** Eine Funktion $f : \mathbb{N} \to \{0, 1\}$ ist computable, wenn es ein Programm gibt, das $f(n)$ für jedes n ausgibt.
- **Theorem:** Es gibt uncomputable Funktionen $\mathbb{N} \to \{0, 1\}$.
- **Implikation:** Programme sind countable, Funktionen uncountable.

Schnell-Check: Abzählbarkeit

- Ist $\mathbb{Z} \times \mathbb{Z}$ countable? Wie?
- Warum ist $\mathbb{R}$ uncountable?

Antworten: Ja, via Cantor's Pairing. $\mathbb{R}$ via Diagonalargument.

Warum Ist Das Wichtig?

Abzählbarkeit hilft uns zu verstehen, was ‘berechenbar’ ist (Programme sind countable, aber Funktionen oft nicht). Es erklärt, warum einige Probleme unlösbar sind.

Uncountable Sets

Übung: Beweise, dass $A = \{f \in \{0,1\}^{\mathbb{N}} \mid f(k) = 0$ falls $k \equiv_2 0\}$ uncountable ist.

Intuition: A ist die Menge aller unendlichen 0-1-Folgen, bei denen die geraden Positionen (0,2,4,...) immer 0 sind. Die ungeraden Positionen (1,3,5,...) können 0 oder 1 sein. Es ist wie Folgen, die "auf den geraden Plätzen leer sind".

Schritt 1

Schritt 1: Injektion finden

Konstruiere $h : \{0,1\}^\infty \to A$. Für jede Folge b, baue $g = h(b)$: Gerade Positionen (0,2,4,...) sind 0. Ungerade Positionen (1,3,5,...) nehmen Bits von b.

Tipp: Wie b in die “Lücken” zwischen geraden Zahlen zu stecken. Einfach: g ist b “verdünnt” mit 0’s dazwischen.

Schritt 2

Schritt 2: Funktion verifizieren

Ist $g \in A$? Ja, da gerade Positionen 0 sind (wie gefordert). Jede b erzeugt genau eine g. Kein Problem!

Schritt 3

Schritt 3: Injektivität beweisen

Wenn $h(b) = h(c)$, dann sind g und g' gleich. Die ungeraden Teile von g kommen direkt von b, also muss $b = c$ sein.

Tipp: Stelle dir zwei gleiche g vor – ihre "ungeraden Bits" müssen gleich sein, also b gleich.

Schritt 4

Schritt 4: Schluss

h ist Injektion, also $\{0,1\}^\infty \preccurlyeq A$. Da $\{0,1\}^\infty$ uncountable, ist A uncountable.

Tipp: Zu viele Folgen, um alle aufzuzählen – wie beim Diagonalargument, wo man immer eine "fehlende" findet.

Äquivalente Mengen

- $A \sim B$: Gleiche "Grösse", auch wenn unendlich.
- **Theorem (Cantor-Bernstein):**
  $A \preccurlyeq B \wedge B \preccurlyeq A \implies A \sim B$.

Beispiel: $(0, 1) \sim \mathbb{R}$ via geometrische Projektion.

Abzählbar vs. Überabzählbar

- Abzählbar: $\preccurlyeq \mathbb{N}$.
- Überabzählbar: Nicht abzählbar, z.B. $\mathbb{R}$.

4-Schritt Muster für Uncountability Beweise:

1. **Injektion finden:** Konstruiere $f : \{0,1\}^\infty \to A$, sodass $b \neq b' \implies f(b) \neq f(b')$.
2. **Funktion verifizieren:** Zeige, dass f well-defined und total ist, und $f(b) \in A$ für alle b.
3. **Injektivität beweisen:** Zeige $f(b) = f(b') \implies b = b'$ oder direkt $b \neq b' \implies f(b) \neq f(b')$.
4. **Schluss:** $\{0,1\}^\infty \preccurlyeq A$. Annahme $A \preccurlyeq \mathbb{N}$ führt zu Widerspruch via Transivität.

Tricks:

- **Complement Trick:** Zeige $A \subseteq B$ (uncountable), $B \setminus A$ countable $\implies$ A uncountable.
- Verwende $\mathbb{R}$ oder $[0,1]$ statt $\{0,1\}^\infty$ falls einfacher.

Cantor's Theorem

- **Theorem:** Für jede Menge A gibt es keine bijektive Funktion $f : A \to \mathcal{P}(A)$.
- **Beweis:** Annahme f bijektiv. Betrachte $B = \{x \in A \mid x \notin f(x)\}$. Dann $B \in \mathcal{P}(A)$, also $f(y) = B$ für ein y. Widerspruch: $y \in B \iff y \notin f(y) = B$.
- **Implikation:** $|\mathcal{P}(A)| > |A|$, Grundlage für Überabzählbarkeit.

Übungsteil: Funktionen & Abzählbarkeit

Übung 1: Funktionseigenschaften (4 Min)

Sei $f : \mathbb{N} \to \mathbb{N}$, $n \mapsto n + 1$. Ist f injektiv, surjektiv, bijektiv?

Lösung zu Übung 1

Injektiv: Ja. Surjektiv: Nein (0 nicht erreicht). Bijektiv: Nein.

Übung 2: Abzählbarkeit beweisen (5 Min)

Beweise, dass die Menge der Punkte mit rationalen Koordinaten ($\mathbb{Q} \times \mathbb{Q}$) abzählbar ist.

Lösung zu Übung 2

Verwende Countability Procedure: Da $\mathbb{Q}$ countable, ist $\mathbb{Q} \times \mathbb{Q}$ countable (Theorem 3.22). Explizit: Finde Injektion $f : \mathbb{Q} \times \mathbb{Q} \to \mathbb{N}$. Identifiziere $\mathbb{Q}$ mit $\mathbb{Z} \times \mathbb{N}^+$ via Brüche, dann $f((p, q)) = 2^{|p|}3^{|q|}$ (FTA-Trick). Bijektion möglich via Pairing.

Übung 3: Uncountability Proof (6 Min)

Beweise, dass für $\ell \geq 1$,
$A_\ell = \{f : \mathbb{N} \to \{0,1\} \mid \sum_{i=0}^{k} f(i) \leq \frac{k}{\ell} + 1 \text{ für alle } k\}$
uncountable ist.
Intuition: A_ℓ ist die Menge aller 0-1-Folgen, bei denen die Anzahl der 1's bis Position k höchstens $\lfloor k/\ell \rfloor + 1$ ist. Das bedeutet, in jedem Block von ℓ Positionen gibt es höchstens eine 1, aber mit etwas Spielraum. Es ist wie Folgen mit "verdünnten" 1's.

Lösung zu Übung 3: Schritt 1

Schritt 1: Injektion finden

Definiere $h_\ell : \{0,1\}^\infty \to A_\ell$. Für Folge b, setze $(h_\ell(b))(n) = b(k)$ wenn $n = k \cdot \ell$, sonst 0.

Tipp: b wird nur an Positionen $0, \ell, 2\ell, \ldots$ platziert, dazwischen 0's. Wie b in weite Abstände zu strecken.

Lösung zu Übung 3: Schritt 2

Schritt 2: Funktion verifizieren

Prüfe, ob $h_\ell(b) \in A_\ell$: Die Summe der 1's bis k ist klein genug (höchstens $\lfloor k/\ell \rfloor + 1$). Ja, weil 1's nur an Vielfachen von ℓ sind.

Lösung zu Übung 3: Schritt 3

Schritt 3: Injektivität beweisen

Wenn $h_\ell(b) = h_\ell(c)$, dann stimmen die Werte an $0, \ell, 2\ell, \ldots$ überein, also $b(k) = c(k)$ für alle k. Also $b = c$.

Tipp: Die "besetzten" Positionen verraten b komplett.

Lösung zu Übung 3: Schritt 4

Schritt 4: Schluss

h_ℓ ist Injektion, also $\{0,1\}^\infty \preccurlyeq A_\ell$. Da $\{0,1\}^\infty$ uncountable, ist A_ℓ uncountable.

Tipp: Zu viele Möglichkeiten für b, unmöglich aufzuzählen – wie beim Diagonalargument.

Übung 4: Kardinalität und Äquivalenz (5 Min)

Sei A uncountable, θ Equivalenzrelation auf A. Beweise, dass A/θ oder $[a]_\theta$ für ein a uncountable ist.

Lösung zu Übung 4

Annahme Widerspruch: A/θ countable, $[a]_\theta$ countable für alle a. Dann $A = \bigcup [a_i]_\theta$ (countable Union countable Mengen, Theorem 3.22), contradiction. Also mindestens eines uncountable.

Übung 5: Uncountability Subset (6 Min)

Beweise, dass $A = \{f \in \{0,1\}^{\mathbb{N}} \mid f(k) = 0 \text{ falls } k \equiv_2 0\}$ uncountable ist.

Lösung zu Übung 5

4-Step Uncountability Pattern:

1. **Injektion:** $f : \{0,1\}^\infty \to A$, $g(k) = 0$ falls k gerade, sonst $b_{\lfloor k/2 \rfloor}$.
2. **Funktion:** $g \in A$ (gerade $k = 0$).
3. **Injektiv:** Falls $b \neq b'$, differieren bei j, dann $g(2j+1) = b_j \neq b'_j$.
4. **Schluss:** $\{0,1\}^\infty \preccurlyeq A$, uncountable.

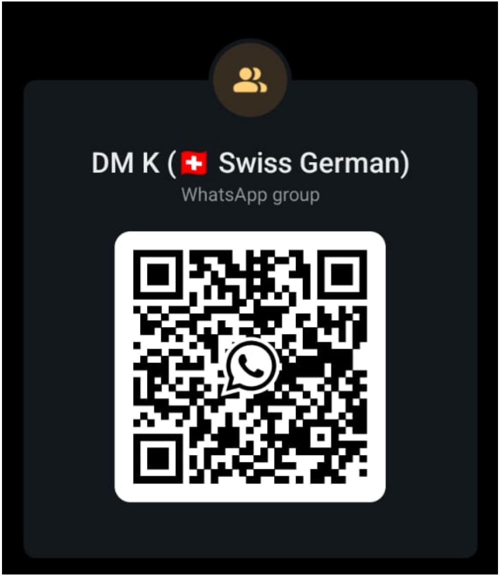
Vorschau auf nächste Woche

Thema: Zahlentheorie (ggT, modulare Arithmetik, RSA)

- Euklidischer Algorithmus
- Kongruenzen
- Anwendungen in Kryptographie

Tipps

- Übe Injektionen und Bijektionen – sie sind Schlüssel zu Abzählbarkeit.
- Visualisiere Diagonalargument mit einer Tabelle.
- Schau Videos zu Cantors Theorem an.


DM K (🇨🇭 Swiss German)
WhatsApp group

Offene Fragen & Feedback

- Fragen zu Funktionen oder Abzählbarkeit?
- Feedback? (https://forms.gle/LPrQfoZNsAHVeKoM9)
- E-Mail: dm@shivi.io

Schöne Woche und bis nächsten Montag!

Appendix: Unberechenbare Funktionen

- Programme sind endlich $\rightarrow$ abzählbar.
- Funktionen $\mathbb{N} \rightarrow \{0, 1\}$ sind überabzählbar.
- $\rightarrow$ Unberechenbare Funktionen existieren (z.B. Halting-Problem).