DM Cheatsheet - Sets, Relations, & Functions - Shivram Sambhus (HS25)

1 Introduction: The Building Blocks of Discrete Structures

This document covers the fundamental concepts of sets, relations, and functions as presented in Chapter 3. It emphasizes procedural understanding, proof construction, and the connections between these abstract structures.

1.1 TOC

2 Part I: Sets (Mengenlehre)

A set is an unordered collection of distinct objects. This is the most fundamental structure in mathematics.

2.1 Core Concepts & Notation

- **Element of:** $x \in A$ ("x is an element of set A").
- **Set-Builder Notation:** $\{x \in U \mid P(x)\}$ ("the set of all x in universe U such that property P(x) is true").
- **Empty Set:** $\emptyset$ or $\{\}$ (the unique set with no elements).
- **Cardinality:** $|A|$ (the number of elements in a finite set A).
- **Power Set:** $\mathcal{P}(A)$ (the set of all subsets of A). If $|A| = n$, then $|\mathcal{P}(A)| = 2^n$.
- **Russell's Paradox:** The "set of all sets that do not contain themselves", $R = \{A \mid A \notin A\}$, leads to a contradiction ($R \in R \Leftrightarrow R \notin R$). This paradox revealed that not every property can define a set. We must start from an existing set, e.g. $\{x \in B \mid P(x)\}$, not $\{x \mid P(x)\}$.

2.2 Proving Set Equality & Subsets

Core Definitions (Axiom of Extensionality)

- **Subset:** $A \subseteq B \equiv \forall x(x \in A \to x \in B)$.
- **Set Equality:** $A = B \equiv \forall x(x \in A \leftrightarrow x \in B) \equiv (A \subseteq B) \land (B \subseteq A)$.

TA Tip: The Element-Chasing Method This is the standard, rigorous way to prove set relations.

1. **To prove $A \subseteq B$:**
   - Start with "Let x be an arbitrary element of A."
   - Use the definition of A to state properties of x.
   - Logically deduce that x must also satisfy the properties of B (using definitions, logic rules).
   - Conclude with "Therefore, $x \in B$."
2. **To prove $A = B$:**
   - First, prove $A \subseteq B$.
   - Then, prove $B \subseteq A$.
   - Conclude that since both inclusions hold, by definition of equality, $A = B$.

Example: Proving a Distributive Law

Claim: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Proof: We prove this by double inclusion.

Part 1: Show $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$

Let $x \in A \cap (B \cup C)$.
1. $\Rightarrow x \in A$ and $x \in (B \cup C)$ (Def. of Intersection)
2. $\Rightarrow x \in A$ and ($x \in B$ or $x \in C$) (Def. of Union)
3. $\Rightarrow$ ($x \in A$ and $x \in B$) or ($x \in A$ and $x \in C$) (Distributive Law of Logic)
4. $\Rightarrow x \in (A \cap B)$ or $x \in (A \cap C)$ (Def. of Intersection)
5. $\Rightarrow x \in (A \cap B) \cup (A \cap C)$ (Def. of Union)

Part 2: Show $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$

Let $x \in (A \cap B) \cup (A \cap C)$.
1. $\Rightarrow x \in (A \cap B)$ or $x \in (A \cap C)$ (Def. of Union)
2. $\Rightarrow$ ($x \in A$ and $x \in B$) or ($x \in A$ and $x \in C$) (Def. of Intersection)
3. $\Rightarrow x \in A$ and ($x \in B$ or $x \in C$) (Factoring out $x \in A$ in logic)
4. $\Rightarrow x \in A$ and $x \in (B \cup C)$ (Def. of Union)
5. $\Rightarrow x \in A \cap (B \cup C)$ (Def. of Intersection)

Since both inclusions hold, the sets are equal by definition.

2.3 Set Operations

Core Operations

- **Union:** $A \cup B = \{x \mid x \in A \lor x \in B\}$
- **Intersection:** $A \cap B = \{x \mid x \in A \land x \in B\}$
- **Difference:** $A \setminus B = \{x \mid x \in A \land x \notin B\}$
- **Cartesian Product:** $A \times B = \{(a, b) \mid a \in A \land b \in B\}$. Creates **ordered pairs**. Note that $A \times B \neq B \times A$ unless $A = B$ or one is empty. The product is not associative: $(A \times B) \times C \neq A \times (B \times C)$.

3 Part II: Relations (Relationen)

A relation describes a relationship between elements of sets. Formally, a binary relation R from a set A to a set B is any subset of the Cartesian product $A \times B$. We write aRb to mean $(a, b) \in R$.

3.1 Operations on Relations

Key Operations

- **Inverse (R^{-1}):** If $R \subseteq A \times B$, then $R^{-1} \subseteq B \times A$. $R^{-1} = \{(b, a) \mid (a, b) \in R\}$.
- **Composition ($S \circ R$):** If $R \subseteq A \times B$ and $S \subseteq B \times C$. $S \circ R = \{(a, c) \mid \exists b \in B, (a, b) \in R \land (b, c) \in S\}$. **Intuition:** A path from a to c through some intermediate b. The order is critical: $S \circ R$ means apply R **then** S. It is associative: $(T \circ S) \circ R = T \circ (S \circ R)$.

3.2 Properties of Relations on a Set A

Property	**Definition ($\forall a, b, c \in A$)**	**Intuition/Graph**
Reflexive	aRa	Every node has a self-loop.
Irreflexive	$a/(R)a$	No node has a self-loop.
Symmetric	$aRb \to bRa$	If there's an edge from a to b, there's one back (all edges are two-way).
Antisymmetric	$(aRb \land bRa) \to a = b$	No two distinct nodes have edges in both directions between them.
Transitive	$(aRb \land bRc) \to aRc$	If there's a path $a \to b \to c$, there's a direct edge $a \to c$. "Shortcut property".

Note: Antisymmetric is **not** the negation of symmetric. A relation can be both (e.g., equality) or neither.

3.3 Special Types of Relations

Equivalence Relation

A relation that is **Reflexive, Symmetric, and Transitive**.
- **Intuition:** Generalizes "equality". It groups similar elements together.
- **Equivalence Class:** $[a]_R = \{x \in A \mid xRa\}$. The set of all elements equivalent to a.
- **Partition:** The set of all equivalence classes of a set A forms a **partition** of A. This means the classes are non-empty, disjoint ($[a]_R \cap [b]_R = \emptyset$ if not aRb), and their union is A.

Partial Order

A relation R that is **Reflexive, Antisymmetric, and Transitive**.
- **Intuition:** Generalizes $\leq$. It defines a hierarchy where some elements may be **incomparable**.
- **Poset:** A pair (A, R) where R is a partial order on A.
- **Comparable vs Incomparable**: Two elements a, b are comparable if aRb or bRa. Otherwise they are incomparable.
- **Total Order:** A partial order where every pair of elements is comparable.
- **Hasse Diagram:** A simplified graph for a finite poset.
  1. Draw nodes for elements.
  2. If b **covers** a (i.e., $a \prec b$ and no c is between them, $a \prec c \prec b$), draw a line from a to b, with b placed higher.

3. Omit self-loops (implied by reflexivity) and transitive edges (implied by transitivity). All edges point "up".

3.4 Elements in Posets

Let $(A, \leq)$ be a poset and $S \subseteq A$.

Minimal & Maximal Elements

- $a \in A$ is **minimal** if no element is smaller: $\neg\exists b \in A, b < a$.
- $a \in A$ is **maximal** if no element is larger: $\neg\exists b \in A, a < b$.

Note: There can be many minimal/maximal elements. In a Hasse diagram, these are the "bottom" and "top" elements.

Least & Greatest Elements

- $a \in A$ is **least** if it's smaller than or equal to all other elements: $\forall b \in A, a \leq b$.
- $a \in A$ is **greatest** if it's greater than or equal to all other elements: $\forall b \in A, b \leq a$.

Note: If they exist, they are unique. A least element is the unique minimal element. A greatest element is the unique maximal element.

Bounds for a Subset S

- **Lower Bound:** $a \in A$ is a lower bound of S if $\forall s \in S, a \leq s$.
- **Upper Bound:** $a \in A$ is an upper bound of S if $\forall s \in S, s \leq a$.
- **Greatest Lower Bound (infimum/meet):** glb(S) or $\inf(S)$ is the greatest of all lower bounds.
- **Least Upper Bound (supremum/join):** lub(S) or $\sup(S)$ is the least of all upper bounds.

Lattices

A poset $(A, \leq)$ is a **lattice** if every pair of elements $\{a, b\}$ in A has a unique meet (glb) and a unique join (lub).

4 Part III: Functions (Funktionen)

A function is a special type of relation that maps each element of a domain to exactly one element of a codomain.

4.1 Definition & Types

Formal Definition

A relation $f \subseteq A \times B$ is a function $f : A \to B$ if it satisfies two conditions:

1. **Totally Defined:** $\forall a \in A, \exists b \in B$ such that $(a, b) \in f$. (Every element in the domain is mapped).
2. **Well-Defined:** If $(a, b) \in f$ and $(a, c) \in f$, then $b = c$. (Each element is mapped to only one output).

- **Image (Range):** $f(S) = \{f(a) \mid a \in S\}$ for a subset $S \subseteq A$. The image of the function is $\mathfrak{I}(f) = f(A)$.
- **Preimage:** $f^{-1}(T) = \{a \in A \mid f(a) \in T\}$ for a subset $T \subseteq B$.

Key Function Types

Type	Formal Definition	Intuition
Injective (one-to-one)	$\forall a_1, a_2 \in A, f(a_1) = f(a_2) \to a_1 = a_2$.	No two inputs map to the same output. No collisions.
Surjective (onto)	$\forall b \in B, \exists a \in A, f(a) = b$.	Every element in the codomain is "hit" by at least one input.
Bijective	Both injective and surjective.	A perfect, one-to-one correspondence between two sets. An inverse function f^{-1} exists if and only if f is bijective.

5 Part IV: Cardinality & Countability

Cardinality provides a way to compare the sizes of sets, including infinite ones, using functions.

5.1 Comparing Set Sizes

Fundamental Definitions

- **Equinumerous ($A \sim B$):** $|A| = |B|$. There exists a **bijection** $f : A \to B$.
- **Dominates ($A \leq B$):** $|A| \leq |B|$. There exists an **injection** $f : A \to B$.
- **Strictly Dominates ($A < B$):** $|A| < |B|$. There is an injection from A to B, but no bijection.

Schröder-Bernstein Theorem

If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$. **Approach:** If you can find an injection from A to B and another injection from B to A, you can conclude a bijection exists without actually constructing it.

5.2 Countable & Uncountable Sets

Definitions

- **Countable:** A set A is countable if it is finite or countably infinite. Formally, $|A| \leq |\mathbb{N}|$.
- **Countably Infinite:** A set A is countably infinite if $|A| = |\mathbb{N}|$. These are sets whose elements can be listed in an infinite sequence (e.g., $a_0, a_1, a_2, \ldots$).
- **Uncountable:** A set that is not countable. Its elements cannot be put into an infinite list.

Key Results & Proof Techniques

- **Countable Sets:** $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{N} \times \mathbb{N}$, the set of all finite-length strings. **Proof Strategy:** To show a set A is countable, find an **injection** from A into a known countable set (like $\mathbb{N}$ or $\mathbb{N} \times \mathbb{N}$).
- **Uncountable Sets:** $\mathbb{R}, \mathcal{P}(\mathbb{N})$, the set of infinite binary sequences $\{0,1\}^\infty$, the interval $[0, 1]$. **Proof Strategy:** Use Cantor's Diagonalization Argument.

Approach: Cantor's Diagonalization Argument Goal: To prove that a set (e.g., infinite binary sequences, $\{0,1\}^\infty$) is uncountable. **Procedure:**

1. **Assume for contradiction** that the set **is** countable. This implies we can create a complete, infinite list of all its elements. $s_0 = b_{0,0}b_{0,1}b_{0,2}\ldots$ $s_1 = b_{1,0}b_{1,1}b_{1,2}\ldots$ $s_2 = b_{2,0}b_{2,1}b_{2,2}\ldots$ $\vdots$
2. **Construct a "diagonal" enemy:** Create a new sequence, s_{new}, that is guaranteed **not** to be on the list. This is done by making its n-th element different from the n-th element of the n-th sequence in the list. The n-th bit of s_{new} is the **flipped** bit of the n-th bit of s_n. $s_{(\text{new})_n} = 1 - b_{n,n}$
3. **Find the contradiction:** The new sequence s_{new} cannot be in our list. Why?
   - It's not s_0 because it differs in the 0-th bit.
   - It's not s_1 because it differs in the 1st bit.
   - In general, it cannot be s_n for any n because it differs in the n-th bit by construction.
4. **Conclusion:** Our list, which was assumed to be complete, is missing an element. This is a contradiction. Therefore, the initial assumption must be false, and the set is uncountable.