Set Theory cheat sheet

Hampus Weslien

May 26, 2017

1 Sets

Cardinality: Cardinality is the number of elements in a set A, written $\#(A)$ or $|A|$. Useful formula for the number of combinations: $\frac{n!}{k!(n-k)!}$

Difference Difference, $x \in A \backslash B$ iff $x \in A$ or $x \in B$

Disjointness Two sets A and B are disjoint if they do not have any common elements: $A \cap B = \emptyset$

Inclusion: Inclusion refers to $A \subseteq B$, this means that if $x \in A$ then $x \in B$

Intersection Intersection, $x \in A \cap B$ iff $x \in A$ or $x \in B$

Poset (partially ordered set): A poset $(A, <)$ is well-founded iff all non-empty subsets $X \subseteq A$ have a minimal element, i.e. for some $m \in X$ and all $a \in X, a \not< m$

Power set The power set of a set A is the set of all its subsets, $P(A) = \{s : s \subseteq A\} = 2^A$

Union: The union, $x \in A \cup B$ iff $x \in A$ or $x \in B$

1.1 Syntax

Generalized union and intersection:

$\bigcup S = \{x : x \in s \text{ for at least one } s \in S\}$
$\bigcap S = \{x : x \in s \text{ for all } s \in S\}$

Example:

$\bigcup\{A_i : i \in I\} \quad \bigcup\{A_i\}_{i\in I} \quad \bigcup_{i\in I} A_i$
$\bigcap\{A_i : i \in I\} \quad \bigcap\{A_i\}_{i\in I} \quad \bigcap_{i\in I} A_i$

List comprehension :

flavor 1	flavor 2
$\{n \in \mathbb{N}^+ : n \text{ is prime}\}$	$\{n : n \in \mathbb{N}^+, n \text{ is prime}\}$
$\{n \in \mathbb{N}^+ \| n \text{ is prime}\}$	$\{2n : n \in \mathbb{N}^+\}$

Families of sets

$\{N_i : i \in \mathbb{N}\}$ with $N_i = \{k \in \mathbb{N} : k \geq i\}$

2 Relations

Antisymmetry: A binary relation $R = A \times A$ is antisymmetric iff for all $a, b \in A$ if aRb and bRa then $a = b$

Asymmetry: A binary relation $R = A \times A$ is asymmetric iff for all $a, b \in A$ if aRb then not bRa

Cartesian product: The (cartesian) product of a pair of sets, or more generally a finite family of sets, is the set of all ordered pairs or n-tuples.

$$A_1 \times ... \times A_n = \{(a_1, ..., a_n) : a_1 \in A_1, ..., a_n \in A_n\}$$

Closure: Given a relation $R \subseteq A \times A$ and a set $X \subseteq A$, the closure of X under R $R[X]$ is defined as the smallest $Y \subseteq A$ such that $X \subseteq Y$ and $R(Y) \subseteq Y$

Closure of relations, rules, generators: Given a set A, a family of relations on A $R = \{R_i \subseteq A^{n_i} : i \in I\}$ and a set $X \subseteq A$, the closure of X under R $R[X]$ is defined as the smallest $Y \subseteq A$ such that $X \subseteq Y$ and $R_i(Y^{n_i}) \subseteq Y$ for all $i \in Y$.

Complement: For a binary relation $R = A \times B$ its complement is the relation

$$\overline{R} = A \times B \backslash R$$

Composition: Given two binary relations $R = A \times B$ and $S = B \times C$ their composition is a binary relation on $A \times C$

$$S \circ R = \{(a, c) : aRb \text{ and } bSc \text{ for some } b \in B\}$$

Converse: For a binary relation $R = A \times B$ its converse (inverse) is the relation

$$R^{-1} = \{(b, a) : aRb\}$$

Equinumerosity principle: $\#(A) = \#(B)$ iff there is some bijection $f : A \to B$

Image: Given a binary relation $R = A \times B$ from A to B, for any $a \in A$ its image under R, written $R(a)$, is defined as $R(a) = \{b \in B : aRb\}$

Irreflexivity: A binary relation $R = A \times A$ is irreflexive iff there is no $a \in A \quad aRa$

N-tupels: $(a_1, ..., a_n) = (b_1, ..., b_n)$ iff $a_i = b_i$ for $i = 1, ..., n$

Order relation, poset: A binary relation $\preceq \subseteq A \times A$ is an (inclusive or non-strict) (partial) order iff it is

1. Reflexive
2. Antisymmetric
3. Transitive

Ordered pairs, tupels: $(a, b) = (x, y)$ iff $a = x$ and $b = y$

Partitions: Given a set A, a partition of A is a set of pairwise disjoint sets $\{B_i : i \in I\}$, such that

$$A = \bigcup_{i \in I} B_i$$

Reflexivity: A binary relation $R = A \times A$ is reflexive iff for all $a \in A \quad aRa$

Similarity relationship: A similarity relationship had two properties,

1. Reflexive
2. Symmetric

Strict (partial) order A binary relation $\prec \subseteq A \times A$ is a strict (partial) order iff it is

1. Irreflexive
2. Transitive

Symmetric closure: The symmetric closure S of a relation R on a set X is given by $S = R \cup \{(x, y) : (y, x) \in R\}$. In other words, the symmetric closure of R is the union of R with its inverse relation, R^{-1}.

Symmetry: A binary relation $R = A \times A$ is symmetric iff for all $a, b \in A$ if aRb then bRa

Total (or linear) order A binary relation $\preceq \subseteq A \times A$ is a (non-strict) total (or linear) order iff it is

1. Irreflexive
2. Antisymmetric
3. Transitive
4. Total (complete): $a \preceq b$ or $b \preceq a$

Transitive clojure: It's the smallest set R* in which R is a subset and we have added relations to make it transitive.

Transivity: A binary relation $R = A \times A$ is transitive iff for all $a, b, c \in A$ if $aRb \wedge bRc \rightarrow aRc$

3 Functions

Bijection: A function $f : A \rightarrow B$ is bijective iff it it is both injective and surjective Notation: $f : A \longleftrightarrow B$

Composition: Given functions $f : A \rightarrow B$ and $g : B \rightarrow C$ their composition $g \circ f : A \rightarrow C$ defines as $g \circ f = g(f(a))$

Closure: Given an endofunction $f : A \rightarrow A$ and a set $X \subseteq A$, the closure of X under f $f[X]$ is defined as the smallest $Y \subseteq A$ such that $X \subseteq Y$ and $F(Y) \subseteq Y$

Equivalence relations: A binary relation $\approx \subseteq A \times A$ is an equivalence relation iff it is

1. Reflexive
2. Symmetric
3. Transitive

Image: Given a function $f : A \rightarrow B$ and a set $X \subseteq A$, the image of X under f is defined as $f(X) = \{f(a) : a \in X\}$

Injection: A function $f : A \rightarrow B$ is injective iff $a \neq b$ implies $f(a) \neq f(b)$ Notation: $f : A \hookrightarrow B$

Inverse: given a function $f : A \rightarrow B$ its inverse (converse) $f^{-1} \subseteq B \times A$ is defined as: $f^{-1} = \{(F(a), a) : a \in A\}$

Restriction of a function: Given a function $f : A \to B$, its restriction to a set $X \subseteq A$ is defined as

$$\begin{array}{cc} f_X : X \to B & f|X \\ a \mapsto f(a) & \text{alternative syntax} \end{array}$$

Set of all functions: B^A $\quad \langle A \to B \rangle$ $\quad \#(B^A) = \#(B)^{\#(A)}$

Surjection: A function $f : A \to B$ is surjective iff $f(A = B)$
Notation: $f : A \twoheadrightarrow B$

4 Notation

Equivalence class: $[x]$ is the equivalence class containing all elements that are considered equal to x in a some predefined relation.

The set of all functions: B^A is the set of all functions from set A to set B

Weird naming :

	$R \subseteq A \times B$	$f : A \to B$
actual values, left	domain	domain
actual values, right	range	range
A	source	domain
B	target	codomain

5 Infinity

Cantor-Schrder-Bernstein theorem (CSB): For ant two sets A and B, if there are two injections $f : A \hookrightarrow B$ and $g : B \hookrightarrow A$ then there exists a bijection $h : B \longleftrightarrow B$
Corollary: if $\#(A) \leq \#(B)$ and $\#(B) \leq \#(A)$ then $\#(A) = \#(B)$

Denumerable: A is denumerable (countable) if it is equinumerous to the natural numbers, i.e. $S \sim \mathbb{N}$
The cardinality of the natural numbers $\#(\mathbb{N}) = \aleph_0$

Finite sequences/strings: Let A be a finite set of n symbols $A = \{a_1, ..., a_n\}$. The set of all finite sequences (strings) of these symbols is A^*. The empty sequence is $\epsilon \in A^*$

Infinite sequences: Let A be a finite set of n symbols $A = \{a_1, ..., a_n\}$. An infinite sequence in A is a function $s : \mathbb{N} \to A$. The set of all infinite sequences in A: $A^{\mathbb{N}}$

Infinity: A is infinite if it is equinumerous to a proper subset of itself. That is, there is some S such that $S \subset A$ and $S \sim A$

Rational numbers: 1 $\mathbb{Q}$ is dense: between any two distinct $r, s \in \mathbb{Q}$ there is $\frac{r+s}{2} \in \mathbb{Q}$

2 Any non-empty open interval $]r, s[\subset \mathbb{Q}$ is equinumerous to $\mathbb{Q}$

Example: Bijection between a subset of the real numbers and the real numbers

$$p_{\mathbb{R}} :]0,1[_{\mathbb{R}} \longleftrightarrow \mathbb{R}$$
$$x \longmapsto \begin{cases} \frac{1}{x} - 2 \text{ for } x < \frac{1}{2} \\ 2 - \frac{1}{x-1} \text{ for } x \geq \frac{1}{2} \end{cases}$$

6 Proofs

Contrapositive proof $(\neg C \implies \neg P)$:

Theorem: If $x^2 - 6x + 5$ is even, then x is odd.

Proof: Suppose x is even. There is an integer a such that $x = 2a.x^2 - 6x + 5 = 4a^2 - 12a + 4 + 1 = 2(2a^2 - 6a + 2) + 1$ So there is an integer b s.t. $x^2 - 6x + 5 = 2b + 1$ Therefore $x^2 - 6x + 5$ is not even.

Direct proof :

Theorem: If x is odd, then x^2 is odd

Proof: Suppose x is odd. Theredore, there is an integer k such that $x = 2k+1$. Thus $x^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$. Note that $2k^2 + 2k$ is an integer. thus there is an integer n such that $x^2 = 2n + 1$. Therefore x^2 is odd.

Direct proof with cases :

Theorem: If $n \in \mathbb{N}$ then $1 + (-1)^n(2n - 1)$ is a multiple of 4.

Proof: Suppose $n \in \mathbb{N}$. Then n is either even or odd.

Case 1: Suppose n is even. Then $n = 2k$ for some $k \in \mathbb{Z}$. Thus $1 + (-1)^{2k}(2(2k) - 1) = 1 + 1^k(4k - 1) = 4k$. That is a multiple of 4.

Case 2: Suppose n is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. Thus $1 + (-1)^{2k+1}(2(2k + 1) - 1) = 1 - (4k + 2 - 1) = -4k$. That is also a multiple of 4.

Proof by contradiction :

Theorem: If $a, b \in \mathbb{Z}$ then $a^2 - 4b \neq 2$

Proof: Suppose there are $a, b \in \mathbb{Z}$ s.t. $a^2 - 4b = 2$. Sinice this implies $a^2 = 4b + 2 = 2(2b + 1)$, a^2 is even. Hence a is even, so $a = 2c$ for some integer c. Thus $4c^2 - 4b = 2$, i.e. $2c^2 - 2b = 1$. Therefore $2(c^2 - b) = 1$ with $c^2 - bin\mathbb{Z}$. So 1 is even.

7 Induction and Recursion

Cumulative (complete) induction :

Hypothesis:	$P(n)$
Basis:	$P(0)$
Induction step:	Assuming that $P(m)$ for all $m < k$ show that $P(k)$

Simple induction :

Hypothesis:	$P(n)$ for all n
Basis:	Show that $P(1)$ (or $P(0)$ or some other, depending on circumstances)
Induction step:	Assuming that $P(k)$ show that $P(k+1)$

Structural induction :

Hypothesis:	$P(x)$ for all $xR[X]$
Basis:	$P(x)$ for all $x \in X$
Induction step:	All rules $R_i \in R$ preserve the property: if their "input" objects have it, then so does their output object.

Structural recursion on domains :

$$R = \{R_1, R_2, R_3\}, \quad C = UTF - 16 \qquad R_1 = \{(s, "-"s) : s \in C^*\}$$
$$V = \{"a" , ... , "z"\} \setminus \{\epsilon\} \qquad R_2 = \{(s_1, s_2, "("s_1" + "s_2")") : s_1, s_2 \in C^*\}$$

$$eval_E : R[V] \to \mathbb{R}$$

$$eval_E : s \mapsto \begin{cases} E(s) & \text{for } s \in V \\ -eval_E(s') & \text{for } s = "-"s' \\ eval_E(s_1) + eval_E(s_2) & \text{for } s = "("s_1"+"s_2")" \\ eval_E(s_1)\dot{e}val_E(s_2) & \text{for } s = "("s_1"*"s_2")" \end{cases}$$

Well-founded induction: Given a well-founded set $(A, <)$ and a property $P(a), a \in A$, if for all $ainA : P(w)$ for all $w < a$ implies $P(a)$ then $P(a)$ for all $a \in A$

Well-founded recursion: Given a well-founded set $(W, <)$and a recursive function definition for a function $f : W \to X$, f is well-defined if it computes the value for every $w \in W$ only depending on values of f for $v < w$.

8 Trees and Graphs

Binary search trees: Given a labelled binary tree (V, R), with labelling function $\lambda : T \to L$ and a totally ordered label set L. It is a binary search tree iff for all nodes their label is greater than any label in their left subtree, and less than any label in their right subtree.

Binary trees: Given a tree (V, R) with root a, we say it is binary if every node has at most two children and there is a labeling function

$$\beta : T\backslash\{a\} \to \{left, right\}$$

such that no two children of the same node are labelled identically.

Cycles: A cycle is a path $a_0, ..., a_n$ where $a_0 = a_n$. A graph that does not contain cycles is called acyclic.

Graphs: A (directed) graph is a pair (V, E) where V is a finite set of vertices (or nodes) and a relation $EsubseteqV \times V$, a set of (directed) edges (or arcs).

Labeled trees: Given a tree (V, R), and a set of labels L, a labelling is a function $\lambda : T \to L$. A tree with a labelling is called a labelled tree

Ordered trees: Given a tree (V, R) with root a, we say it is ordered if there is a function

$$\mu : T \backslash \{a\} \rightarrow \mathbb{N}^+$$

such that for every node its n children are labelled $1...n$.

Paths: Given a graph (V, E), a path is a finite sequence $a_0, ..., a_n$ in V with $n \geq 1$ such that for .The length of the path is n.

Spanning trees: Given an undirected graph (T, S), an unrooted tree (T, R) is a spanning tree for it iff $RsubseteqS$

Trees: A (rooted) tree is a graph (T, R) such that T is empty or there is an $a \in T$ such that:

(i) for every $x \in T, x \neq a$ there is exactly one path from a to x

(ii) there is no path from a to a.

Properties:

1 Any non-empty tree has a unique root.

2 A root has no parent.

3 Every non-root has exactly one parent.

4 A tree with n nodes has n-1 links

5 A tree contains no cycles.

Undirected graphs: An (undirected) graph is a pair (V, E) where V is a set of vertices (or nodes) and a symmetric relation $EsubseteqV \times V$, a set of (undirected) edges (or arcs).

Unrooted trees: A structure (V, S) is an unrooted (undirected)tree iff (V, R) is a rooted tree and S is the symmetric closure of R.

Defining trees recursively :

1 The empty graph $(\emptyset, \emptyset)$ is a tree.

2 Given a family of disjoint trees $(T_i, R_i)_i = 1$..n, i.e. $T_i \cap T_j = \emptyset$ when $i \neq j$, and with roots $B = \{b_i : 1 \leq i \leq n\}$, as well as a fresh $a \notin \bigcup_{i \in 1..n} R_i$ we can create a new tree with root a:

9 Propositional Logic

Assignments and valuations: Given a set of elementary letters E and an assignment v, a valuation is the recursive extension of v over the set F[E] of formulae in E generated by a set of rules F:

$$v^{+}F[E] \to \{1, 0\}$$

Tautological implication: Given a set of formulae A and a formula β we say that A tautologically implies β if there is no valuation v such that

$$v(\alpha) = 1 \text{ for all } \alpha \in A \text{ and } v(\beta) = 0$$

$$A \models B \qquad A \vdash B$$

Tautological equivalence: Given two formulae α and β, we say that they are tautologically equivalent if they tautologically imply each other.

$$\alpha \dashv\vdash \beta$$

Name	LHS	RHS
Double negation	α	$\neg\neg\alpha$
Commutation for $\wedge$	$\alpha\wedge\beta$	$\beta\wedge\alpha$
Association for $\wedge$	$\alpha\wedge(\beta\wedge\gamma)$	$(\alpha\wedge\beta)\wedge\gamma$
Commutation for $\vee$	$\alpha\vee\beta$	$\beta\vee\alpha$
Association for $\vee$	$\alpha\vee(\beta\vee\gamma)$	$(\alpha\vee\beta)\vee\gamma$
Distribution of $\wedge$ over $\vee$	$\alpha\wedge(\beta\vee\gamma)$	$(\alpha\wedge\beta)\vee(\alpha\wedge\gamma)$
Distribution of $\vee$ over $\wedge$	$\alpha\vee(\beta\wedge\gamma)$	$(\alpha\vee\beta)\wedge(\alpha\vee\gamma)$
Absorption	α	$\alpha\wedge(\alpha\vee\beta)$
	α	$\alpha\vee(\alpha\wedge\beta)$
Expansion	α	$(\alpha\wedge\beta)\vee(\alpha\wedge\neg\beta)$
	α	$(\alpha\vee\beta)\wedge(\alpha\vee\neg\beta)$
de Morgan	$\neg(\alpha\wedge\beta)$	$\neg\alpha\vee\neg\beta$
	$\neg(\alpha\vee\beta)$	$\neg\alpha\wedge\neg\beta$
	$\alpha\wedge\beta$	$\neg(\neg\alpha\vee\neg\beta)$
	$\alpha\vee\beta$	$\neg(\neg\alpha\wedge\neg\beta)$
Limiting cases	$\alpha\wedge\neg\alpha$	$\beta\wedge\neg\beta$
	$\alpha\vee\neg\alpha$	$\beta\vee\neg\beta$

Table 8.8 Some important tautological equivalences using $\to$, $\leftrightarrow$

Name	LHS	RHS
Contraposition	$\alpha\to\beta$	$\neg\beta\to\neg\alpha$
	$\alpha\to\neg\beta$	$\beta\to\neg\alpha$
	$\neg\alpha\to\beta$	$\neg\beta\to\alpha$
Import/export	$\alpha\to(\beta\to\gamma)$	$(\alpha\wedge\beta)\to\gamma$
	$\alpha\to(\beta\to\gamma)$	$\beta\to(\alpha\to\gamma)$
Consequential mirabilis (miraculous consequence)	$\alpha\to\neg\alpha$	$\neg\alpha$
	$\neg\alpha\to\alpha$	α
Commutation for $\leftrightarrow$	$\alpha\leftrightarrow\beta$	$\beta\leftrightarrow\alpha$
Association for $\leftrightarrow$	$\alpha\leftrightarrow(\beta\leftrightarrow\gamma)$	$(\alpha\leftrightarrow\beta)\leftrightarrow\gamma$
$\neg$ through $\leftrightarrow$	$\neg(\alpha\leftrightarrow\beta)$	$\alpha\leftrightarrow\neg\beta$
Translations between connectives	$\alpha\leftrightarrow\beta$	$(\alpha\to\beta)\wedge(\beta\to\alpha)$
	$\alpha\leftrightarrow\beta$	$(\alpha\wedge\beta)\vee(\neg\alpha\wedge\neg\beta)$
	$\alpha\to\beta$	$\neg(\alpha\wedge\neg\beta)$
	$\alpha\to\beta$	$\neg\alpha\vee\beta$
	$\alpha\vee\beta$	$\neg\alpha\to\beta$
Translations of negations of connectives	$\neg(\alpha\to\beta)$	$\alpha\wedge\neg\beta$
	$\neg(\alpha\wedge\beta)$	$\alpha\to\neg\beta$
	$\neg(\alpha\leftrightarrow\beta)$	$(\alpha\wedge\neg\beta)\vee(\beta\wedge\neg\alpha)$

10 Quantificational Logic

Free and bound variable occurrences: A variable occurrence is bound iff it occurs inside the scope of a quantifier that binds that variable. It is free otherwise.

A formula with no free variable occurrences is called closed. A closed formula is a sentence.

Logic with quantifiers (informally): logic with quantifiers (informally)

$\forall x(\alpha)$ represents forall x, α alt. notation $\bigwedge_x \alpha$

$\exists x(\alpha)$ represents there exists an x, such that α alt. notation $\bigvee_x \alpha$

Quantifier scopes: