

# Discreet Math Notes

Samuel Lindskog

December 10, 2023

## 1 Basic Terms, laws, and concepts

### 1.1 Laws of Statements

DeMorgan's laws

$$\neg(P \wedge Q) \equiv \neg P \vee \neg Q$$

$$\neg(P \vee Q) \equiv \neg P \wedge \neg Q$$

Commutative laws

$$P \wedge Q \equiv Q \wedge P$$

$$P \vee Q \equiv Q \vee P$$

Associative laws

$$P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$$

$$P \vee (Q \vee R) \equiv (P \vee Q) \vee R$$

Idempotent laws

$$P \wedge P \equiv P$$

$$P \vee P \equiv P$$

Distributive laws

$$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$$

$$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$$

Absorption laws

$$P \vee (P \wedge Q) \equiv P$$

$$P \wedge (P \vee Q) \equiv P$$

$(P \wedge Q)$  is always false when  $\neg P$

$(P \vee Q)$  is always true when  $P$

Double Negation law

$$\neg\neg P \equiv P$$

## Tautology laws

A tautology is a statement that is always true

$$\begin{aligned}P \wedge (\text{tautology}) &\equiv P \\P \vee (\text{tautology}) &\equiv \text{tautology} \\\neg(\text{tautology}) &\equiv \text{contradiction}\end{aligned}$$

## Contradiction laws

A contradiction is a statement that is always false

$$\begin{aligned}P \wedge (\text{contradiction}) &\equiv \text{contradiction} \\P \vee (\text{contradiction}) &\equiv P \\\neg(\text{contradiction}) &\equiv \text{tautology}\end{aligned}$$

## Modus Ponens and Modus Tollens

$$\begin{aligned}(P \Rightarrow Q) \wedge P &\Rightarrow Q \text{ modus ponens} \\(P \Rightarrow Q) \wedge \neg Q &\Rightarrow P \text{ modus tollens}\end{aligned}$$

## 1.2 Free and Unbound variables

In the statement  $y \in \{x \mid P(x)\}$ ,  $y$  is the *free variable* and  $x$  is the *bound variable*. The free variables stand for objects the statement says something about. Bound variables are letters used for their convenience in expressing ideas, and should not be thought of as standing for any particular object. Statements with only bound variables are just objects, but statements with free variables can be true or false.

## 1.3 Universe of discourse

When a statement contains variables, the *universe of discourse* is the set of all values the variables can take on, and we say that these variables *range over* this universe. For example, suppose  $P(x)$  is a statement, with the variable  $x$  ranging over universe  $U$ . Then, the truth set of  $P(x)$  with universe  $U$  is  $\{x \in U \mid P(x)\}$ , which can be stated implicitly as  $\{x \mid P(x)\}$ .

## 1.4 Truth set

The truth set of a statement  $P(x)$  is the set of all  $x$  in the universe of discourse that make the statement  $P(x)$  true i.e.

$$\text{The truth set of } P(x) \equiv \{x \mid P(x)\}$$

$P(y)$  can also be written in its equivalent forms

$$y \in \{x \mid P(x)\} \equiv P(y)$$

**Example:**

$$y \in \{x \in \mathbb{R} \mid x < 3\} \equiv y \in \mathbb{R} \wedge y < 3$$

## 1.5 Standard sets

$\mathbb{N}$

The set of natural numbers  $\{1, 2, 3, \dots\}$

$\mathbb{W}$

The set of whole numbers  $\{0, 1, 2, 3, \dots\}$

$\mathbb{Z}$

The set of integers  $\{\dots, -1, 0, 1, \dots\}$

$\mathbb{Q}$

The set of rational numbers  $\{\frac{a}{b} | a, b \in \mathbb{Z}, b \neq 0\}$

$\mathbb{R}$

The set of real numbers

**Irrational numbers**

$$\{x \in \mathbb{R} \mid x \notin \mathbb{Q}\}$$

**Even numbers**

$$\{x \in \mathbb{Z} \mid x = 2m, m \in \mathbb{Z}\}$$

**Odd numbers**

$$\{x \in \mathbb{Z} \mid x = 2m + 1, m \in \mathbb{Z}\}$$

## 1.6 Cardinality

The cardinality of a finite set  $S$  is the number of elements in  $S$ , denoted  $|S|$

**Cardinality of unions**

$$|S \cup T| = |S| + |T| - |S \cap T|$$

## 1.7 Empty set

The empty set  $\emptyset$ , equivalent to  $\{\}$ , is a *subset* ( $\subseteq$ ) of any set, but not an *element* ( $\in$ ) of every set.

## 1.8 Collections and Families

A collection or family (both mean the same thing) is a set of sets, e.g.  $\{\{2, 3, 4\}, \{2, 1, 3\}\}$ . Usually represented with capital script letters, e.g.  $\mathcal{L}$ . Can also be indexed  $\{S_k | k \in I\}$

## 1.9 Power set

The collection of all subsets of  $S$  is called the power set of  $S$ , denoted:  $\mathcal{P}(S) = \{A \mid A \subseteq S\}$

### 1.10 Intesection and union

Intersection:  $A \cap B$ , i.e.  $\{x \mid x \in A \wedge x \in B\}$

Union:  $A \cup B$ , i.e.  $\{x \mid x \in A \vee x \in B\}$

Complement,  $A^c$ , Difference set:  $A \setminus B$ , i.e.  $\{x \mid x \in A \wedge x \notin B\}$

Symmetric difference of  $A$  and  $B$ ,  $A \Delta B$ :  $(A \cup B) \setminus (A \cap B) \equiv (A \setminus B) \cup (B \setminus A)$

**Collections and Families**

$$\bigcap_{i \in I} S_i \equiv \{x \mid \forall i \in I, x \in S_i\}$$

$$\bigcup_{i \in I} S_i \equiv \{x \mid \exists i \in I, x \in S_i\}$$

$$\bigcap \mathcal{F} \equiv \{x \mid \forall X \in \mathcal{F} (x \in X)\}$$

### 1.11 Disjoint sets

Sets  $A$  and  $B$  are disjoint if  $A \cap B = \emptyset$

### 1.12 Laws of sets and collections

**Distributive laws**

$$\begin{aligned}A \cup (B \cap C) &= (A \cap B) \cup (A \cap C) \\A \cap (B \cup C) &= (A \cup B) \cap (A \cup C)\end{aligned}$$

**Demorgan's laws**

$$\begin{aligned}\neg(A \cap B) &= \neg A \cup \neg B \\ \neg(A \cup B) &= \neg A \cap \neg B\end{aligned}$$

$$\begin{aligned}\left(\bigcup_{i \in I} S_i\right)^c &= \bigcap_{i \in I} S_i^c \\ \left(\bigcap_{i \in I} S_i\right)^c &= \bigcup_{i \in I} S_i^c\end{aligned}$$

### 1.13 Cartesian product

$$\begin{aligned}A \times B &= \{(a, b) \mid a \in A, b \in B\} \\ S_1 \times S_2 \times \dots \times S_n &= \{(s_1, s_2, \dots, s_n) \mid s_1 \in S_1, s_2 \in S_2, \dots, s_n \in S_n\} \\ &= \prod_{i=1}^n S_i\end{aligned}$$

### 1.14 Partitions

A partition of a nonempty set  $S$  is a collection  $\mathcal{L}$  of nonempty mutually disjoint subsets  $B_i$  such that:

$$\mathcal{L} = \{B_i \mid i \in I\} \text{ and } \bigcup_{i \in I} B_i = S$$

The sets  $B_i$  are called blocks of the partition.

### 1.15 Quantifiers

**Universal quantifier**

The universal quantifier is  $\forall$ . The statement  $\forall x P(x)$  means  $P(x)$  is true for all  $x \in U$ , i.e.  $\{x \in U \mid P(x)\} = U$  is true.

**Existential quantifier**

The existential quantifier is  $\exists$ . The statement  $\exists x P(x)$  means that there exists  $x \in U$  such that  $P(x)$ , i.e.  $\{x \in U \mid P(x)\} \neq \emptyset$  is true.

**Unique existence**

$$\exists! x P(x) \equiv \exists x (P(x) \wedge \neg \exists y (P(y) \wedge x \neq y))$$

## Quantifier negation laws

$$\neg \exists x P(x) \equiv \forall x \neg P(x)$$

$$\neg \forall x P(x) \equiv \exists x \neg P(x)$$

## Commutativity of quantifiers

Like quantifiers are commutative. For example,  $\exists y \exists x \equiv \exists x \exists y$  and  $\forall y \forall x \equiv \forall x \forall y$ .

## 1.16 Subsets

$$A \subseteq B \Rightarrow \forall x (x \in A \Rightarrow x \in B)$$

## 1.17 Implication

$Q$  implies  $P$

$$Q \Rightarrow P$$

If *antecedent*  $P$ , then *consequence*  $Q$ .

$$P \Rightarrow Q$$

Converse

$$\neg P \Rightarrow \neg Q$$

Contrapositive

The double implication  $\Leftrightarrow$ , otherwise known as *iff*, can be expressed as  $P \Leftrightarrow Q \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P)$

# 2 Proof catagories

## Direct proof

Assuming antecedent  $P$ , prove consequence  $Q$

$$P \Rightarrow Q$$

## Indirect Proof

Indirect proofs consist of two proof types: proof by contrapositive, and proof by contradiction. Both start by assuming the consequence is false, and using it as the antecedent. Proof by contrapositive proves the antecedent must be false following a false consequence ( $\neg Q \Rightarrow \neg P$ ), and proof by contradiction proves a false consequence contradicts a true antecedent ( $\neg Q \Rightarrow \text{false}$ ). Indirect Proofs are often suitable when dealing with concepts defined in terms of negations, such as "infinite" (not finite), "irrational" (not rational), and "prime", ( $\neq 1$  and not composite).

## Existence and uniqueness proofs

### Tips and tricks

Begin by stating the antecedents in a way logically equivalent (directly, or contrapositively) to the implication you are proving. Expand from there until you reach the desired consequence. Then restate that the antecedent implies the consequence. Lastly, if the antecedents are different than those of the original implication, explain how the proved implication is logically equivalent to the original implication, e.g. "the theorem follows by the logical equivalence of the implication and its contrapositive".

## Proofs involving quantifiers

A universal quantifier specifies for all  $x$ ,  $P(x)$ , and prove  $P(x)$ . Example: Let  $x$  be arbitrary (prove  $P(x)$ ). Then for all  $x$ ,  $P(x)$ . Don't put restrictions on  $x$ , givens should only aid in understanding how the objects in the goal relate to each other.

