

COMP0147 Discrete Mathematics for Computer Scientists Notes

Joe

March 28, 2019

Notes adapted from lecture notes by Max Kanovich and Robin Hirsch [1].

Contents

1	Foundations	5
1.1	Set Theory	5
1.1.1	Set Notations	5
1.1.2	Properties	5
1.1.3	Set Equality	6
1.1.4	Set Operations	6
1.1.5	Boolean Algebra	6
1.1.6	Set Algebra	7
1.2	Functions	9
1.2.1	Composition of Injections	10
1.2.2	Composition of Surjection	10

1 Foundations

Contents

1.1 Set Theory	5
1.1.1 Set Notations	5
1.1.2 Properties	5
1.1.3 Set Equality	6
1.1.4 Set Operations	6
1.1.5 Boolean Algebra	6
1.1.6 Set Algebra	7
1.2 Functions	9
1.2.1 Composition of Injections	10
1.2.2 Composition of Surjection	10

1.1 Set Theory

1.1.1 Set Notations

- Set definition: $A = \{a, b, c\}$
- Set membership (element-of): $a \in A$
- Set builder notation: $\{x \mid x \in \mathbb{R} \wedge x^2 = x\}$
- Empty set: \emptyset

1.1.2 Properties

- No structure
- No order
- No copies

For example, a, b, c are references to actual objects in

$$\{a, b, c\} \Leftrightarrow \{c, a, b\} \Leftrightarrow \{a, b, c, b\}$$

1.1.3 Set Equality

Definition 1.1.1 (Set Equality). Set $A = B$ iff:

1. $A \subseteq B \implies \forall x(x \in A \rightarrow x \in B)$
2. $B \subseteq A \implies \forall y(y \in B \rightarrow y \in A)$

Remark. $A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$

1.1.4 Set Operations

- *Union:* $A \cup B \equiv \{x \mid x \in A \vee x \in B\}$
- *Intersection:* $A \cap B \equiv \{x \mid x \in A \wedge x \in B\}$
- *Relative Complement:* $A \setminus B \equiv \{x \mid x \in A \wedge x \notin B\}$
- *Absolute Complement:* $A^c \equiv U \setminus A \equiv \{x \mid x \in U \wedge x \notin A\}$
- *Symmetric Difference:* $A \Delta B \equiv (A \setminus B) \cup (B \setminus A) \equiv (A \cup B) \setminus (A \cap B)$
- *Cartesian Product:* $A \times B \equiv \{(x, y) \mid x \in A \wedge y \in B\}$

1.1.5 Boolean Algebra

Definition 1.1.2 (De Morgan's Laws).

$$\neg(p \vee q) \equiv \neg p \wedge \neg q \quad (1.1)$$

$$\neg(p \wedge q) \equiv \neg p \vee \neg q \quad (1.2)$$

Definition 1.1.3 (Idempotent Laws).

$$p \vee p \equiv p \quad (1.3)$$

$$p \wedge p \equiv p \quad (1.4)$$

Definition 1.1.4 (Commutative Laws).

$$p \vee q \equiv q \vee p \quad (1.5)$$

$$p \wedge q \equiv q \wedge p \quad (1.6)$$

Definition 1.1.5 (Associative Laws).

$$p \vee (q \vee r) \equiv (p \vee q) \vee r \quad (1.7)$$

$$p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r \quad (1.8)$$

Definition 1.1.6 (Distributive Laws).

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r) \quad (1.9)$$

$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r) \quad (1.10)$$

Definition 1.1.7 (Identity Laws).

$$p \vee F \equiv p \quad (1.11)$$

$$p \vee T \equiv T \quad (1.12)$$

$$p \wedge T \equiv p \quad (1.13)$$

$$p \wedge F \equiv F \quad (1.14)$$

Definition 1.1.8 (Absorption Laws).

$$p \vee (p \wedge q) \equiv p \quad (1.15)$$

$$p \wedge (p \vee q) \equiv p \quad (1.16)$$

Definition 1.1.9 (Implication and Negation Laws).

- *Identity:* $p \rightarrow q \equiv \neg p \vee q$
- *Counter-example:* $\neg(p \rightarrow q) \equiv p \wedge \neg q$
- *Equivalences:* $p \rightarrow q \rightarrow r \equiv (p \wedge q) \rightarrow r \equiv q \rightarrow (p \rightarrow r)$
- *Absorption:*
 - $p \rightarrow T \equiv T$
 - $p \rightarrow F \equiv \neg p$
 - $T \rightarrow p \equiv p$
 - $F \rightarrow p \equiv T$
- *Contrapositive:* $p \rightarrow q \equiv \neg q \rightarrow \neg p$
- *Law of Excluded Middle:*
 - $p \vee \neg p \equiv T$
 - $p \wedge \neg p \equiv F$
- *Double Negation:* $\neg\neg p \equiv p$
- *Reduction to Absurdity:* $\neg p \rightarrow F \equiv p$

1.1.6 Set Algebra

Definition 1.1.10 (De Morgan's Laws).

$$(A \cup B)^c \equiv A^c \cap B^c \quad (1.17)$$

$$(A \cap B)^c \equiv A^c \cup B^c \quad (1.18)$$

Definition 1.1.11 (Idempotent Laws).

$$A \cup A \equiv A \quad (1.19)$$

$$A \cap A \equiv A \quad (1.20)$$

Definition 1.1.12 (Commutative Laws).

$$A \cup B \equiv B \cup A \quad (1.21)$$

$$A \cap B \equiv B \cap A \quad (1.22)$$

Definition 1.1.13 (Associativity Laws).

$$A \cup (B \cup C) \equiv (A \cup B) \cup C \quad (1.23)$$

$$A \cap (B \cap C) \equiv (A \cap B) \cap C \quad (1.24)$$

Definition 1.1.14 (Distributive Laws).

$$A \cap (B \cup C) \equiv (A \cap B) \cup (A \cap C) \quad (1.25)$$

$$A \cup (B \cap C) \equiv (A \cup B) \cap (A \cup C) \quad (1.26)$$

Definition 1.1.15 (Identity Laws).

$$A \cup \emptyset \equiv A \quad (1.27)$$

$$A \cap \emptyset \equiv \emptyset \quad (1.28)$$

$$A \cap U \equiv A \quad (1.29)$$

$$A \cup U \equiv U \quad (1.30)$$

Definition 1.1.16 (Absorption Laws).

$$A \cup (A \cap B) \equiv A \quad (1.31)$$

$$A \cap (A \cup B) \equiv A \quad (1.32)$$

Definition 1.1.17 (Difference Identity Laws).

$$C \setminus (A \cup B) \equiv (C \setminus A) \cap (C \setminus B) \quad (1.33)$$

$$C \setminus (A \cap B) \equiv (C \setminus A) \cup (C \setminus B) \quad (1.34)$$

Definition 1.1.18 (Complement-Difference Identity Law).

$$C \setminus D \equiv C \cap D^c \quad (1.35)$$

Definition 1.1.19 (Double Complement Law).

$$(D^c)^c \equiv D \quad (1.36)$$

Definition 1.1.20 (Contraposition).

$$C \subseteq D \Leftrightarrow D^c \subseteq C^c \quad (1.37)$$

$$C = D \Leftrightarrow C^c = D^c \quad (1.38)$$

Definition 1.1.21 (Arbitrary Union). Given sets A_1, A_2, \dots, A_n where $I = \{1, 2, \dots, n\}$

$$A_1 \cup A_2 \cup \dots \cup A_n \equiv \bigcup_{i \in I} A_i \quad (1.39)$$

Then

$$x \in \bigcup_{i \in I} A_i \Leftrightarrow \exists i \in I: x \in A_i \quad (1.40)$$

Definition 1.1.22 (Arbitrary Intersection). Given sets A_1, A_2, \dots, A_n where $I = \{1, 2, \dots, n\}$

$$A_1 \cap A_2 \cap \dots \cap A_n \equiv \bigcap_{i \in I} A_i \quad (1.41)$$

Then

$$x \in \bigcap_{i \in I} A_i \Leftrightarrow \forall i \in I: x \in A_i \quad (1.42)$$

1.2 Functions

Definition 1.2.1 (Function). A function f is a mapping from X to Y

$$f: X \mapsto Y \quad (1.43)$$

- $\text{domain}(f) = X$
- $\text{image}(f) = f(X)$

Definition 1.2.2 (Total Function). A function is *total* if

$$\text{domain}(f) = X \quad (1.44)$$

Definition 1.2.3 (Partial Function). A function is *partial* if

$$\text{domain}(f) \subseteq X \quad (1.45)$$

Definition 1.2.4 (Surjection). A function $f: X \mapsto Y$ is *surjective* iff

$$f(X) = Y \Leftrightarrow \forall y \in Y: \exists x \in X: f(x) = y \quad (1.46)$$

Namely each $y \in Y$ has a corresponding $x \in X$.

Definition 1.2.5 (Injection (Encodings, One-to-one)). A function $f: X \mapsto Y$ is *injective* iff

$$\forall x_1, x_2 \in X: x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2) \quad (1.47)$$

$$\Leftrightarrow \forall x_1, x_2 \in X: f(x_1) = f(x_2) \rightarrow x_1 = x_2 \quad (1.48)$$

Namely each distinct element $x \in X$ maps to a different element in Y .

Definition 1.2.6 (Bijection). A function $f: X \mapsto Y$ is *bijective* iff f is both *injective* and *surjective*.

$$\text{Bijective}(f) \equiv \text{Injective}(f) \wedge \text{Surjective}(f) \quad (1.49)$$

The *inverse bijection* $f^{-1}: Y \mapsto X$ does exist.

1.2.1 Composition of Injections

Proposition 1.2.1 (Composition of Injection). Given *injections* $f: X \mapsto Y$ and $g: Y \mapsto Z$, then their *composition* $h: X \mapsto Z$ is given by

$$h(x) = g(f(x)) \quad (1.50)$$

Then h is also an *injective* function. Namely $h = g \circ f$ where h is composed from g and f with f applied first.

Proof. Given any $x_1, x_2 \in X$ where $x_1 \neq x_2$, then

$$f(x_1) \neq f(x_2) \quad (1.51)$$

as f is *injective*, and thus

$$h(x_1) = g(f(x_1)) \neq g(f(x_2)) = h(x_2) \quad (1.52)$$

h is *injective* consequently. ■

1.2.2 Composition of Surjection

Proposition 1.2.2 (Composition of Surjection). Given *surjections* $f: X \mapsto Y$ and $g: Y \mapsto Z$, then their *composition* $h: X \mapsto Z$ is given by

$$h(x) = g(f(x)) \quad (1.53)$$

Then h is also an *surjective* function.

Proof. To prove $h: X \mapsto Z$ is *injective*, it is required to prove that

$$\forall z \in Z: \exists x \in X: h(x) = z \quad (1.54)$$

Where $h(x) \Leftrightarrow (g \circ f)(x) \Leftrightarrow g(f(x))$.

Since for all elements $z \in Z$ ($\forall z \in Z$):

1. That $g: Y \mapsto Z$ is *surjective* by definition, then $\exists y \in Y: g(y) = z$.

2. That $f: X \mapsto Y$ is *surjective* by definition, then $\exists x \in X: f(x) = y$.

Then $\forall z \in Z: \exists x \in X: h(x) = (g \circ f)(x) = g(f(x)) = g(y) = z$ holds true. ■

Bibliography

- [1] Max Kanovich and Robin Hirsch.
“Lecture Notes on Discrete Mathematics for Computer Scientists”.
URL: http://www.cs.ucl.ac.uk/1819/a4u/t2/comp0147_discrete_mathematics_for_computer_scientists/.