Fundamentals of Mathematics Lecture 3: Mathematical Notation

Guan-Shieng Huang

National Chi Nan University, Taiwan

Spring, 2008

Greek Letters I

1. A, α, Alpha
2. B, β, Beta
3. Γ, γ, Gamma
4. Δ, δ, Delta
5. E, ϵ, Epsilon
6. Z, ζ, Zeta
7. H, η, Eta
8. Θ, θ, Theta
9. I, ι, Iota
10. K, κ, Kappa
11. Λ, λ, Lambda
12. M, μ, Mu

Greek Letters II

13. N, ν, Nu
14. Ξ, ξ, Xi
15. O, o, Omicron
16. Π, π, Pi
17. P, ρ, Rho
18. Σ, σ, Sigma
19. T, τ, Tau
20. Υ, υ, Upsilon
21. Φ, ϕ, Phi
22. X, χ, Chi
23. Ψ, ψ, Psi
24. Ω, ω, Omega

Logic I

- Conjunction: $p \wedge q$, $p \cdot q$, $p \& q$ (p and q)
- Disjunction: $p \vee q$, $p + q$, $p | q$ (p or q)
- Conditional: $p \rightarrow q$, $p \Rightarrow q$, $p \supset q$ (p implies q)
- Biconditional: $p \leftrightarrow q$, $p \Leftrightarrow q$ (p if and only if q)
- Exclusive-or: $p \oplus q$, $p + q$
- Universal quantifier: $\forall$ (for all)
- Existential quantifier: $\exists$ (there is, there exists)
- Unique existential quantifier: $\exists!$

Logic II

- $p \longrightarrow q \equiv \neg p \vee q$
- $\neg(p \vee q) \equiv \neg p \wedge \neg q$, $\neg(p \wedge q) \equiv \neg p \vee \neg q$
- $\neg\forall_x P(x) \equiv \exists_x \neg P(x)$, $\neg\exists_x P(x) \equiv \forall_x \neg P(x)$
- $\forall_x \exists_y P(x, y) \not\equiv \exists_y \forall_x P(x, y)$ in general
- $p \oplus q \equiv (p \wedge \neg q) \vee (\neg p \wedge q)$

Set Theory I

- Empty set: $\emptyset$, $\{\}$
- roster: $S = \{a_1, a_2, \ldots, a_n\}$
  defining predicate: $S = \{x | \ P(x)\}$ where P is a predicate
  recursive description
- $\mathbb{N}$: natural numbers
  $\mathbb{Z}$: integers
  $\mathbb{R}$: real numbers
  $\mathbb{C}$: complex numbers
- Two sets A and B are equal if $x \in A \Leftrightarrow x \in B$.
  $A \subseteq B$: $\forall_x [x \in A \Rightarrow x \in B]$
- $|A|$: the cardinality of A (size of A)
  (We will discuss infinite sets in a latter lecture)
  $|A \cup B| = |A| + |B| - |A \cap B|$ for finite sets

Set Theory II

- multiset: counts the duplication of each element
  (Unfortunately, it uses the same notation $\{\ldots\}$)
- $\bigcap_{i\in I} A = \{x \mid x \in A_i \text{ for all } i \in I\}$
- $\bigcup_{i\in I} A = \{x \mid x \in A_i \text{ for some } i \in I\}$
- $A \times B$: $\{(a,b) \mid a \in A \text{ and } b \in B\}$ (the Cartesian product)
- $\overline{A}$ or A^c: $U - A$ where U is the universe (the complement)
- $A - B = A \backslash B = \{x \mid x \in A \text{ but } x \notin B\}$ (set difference)
- $\mathcal{P}(A)$ or 2^A: the set of all subsets of A (the power set)
  $|A| < |\mathcal{P}(A)|$ for all sets

Functions I

- $f : A \to B$ (f maps to B)
  $y = f(x)$ written as $f : x \mapsto y$
- injection (one-to-one), surjection (onto), bijection (one-to-one and onto)
- Let $S_1, S_2 \subseteq A$ and $T_1, T_2 \subseteq B$
  $f(S_1 \cup S_2) = f(S_1) \cup f(S_2)$
  $f(S_1 \cap S_2) \subseteq f(S_1) \cap f(S_2)$
  $f(\overline{S_1}) \supseteq \overline{f(S_1)}$
  $f^{-1}(T_1 \cup T_2) = f^{-1}(T_1) \cup f^{-1}(T_2)$
  $f^{-1}(\overline{T_1}) = \overline{f^{-1}(T_1)}$
  $f^{-1}(f(S_1)) \supseteq S_1$
  $f(f^{-1}(T_1)) \subseteq T_1$

Functions II

- $f : A \to B$, $g : B \to C$ are both bijection
  $\Rightarrow (g \circ f)^{-1} = f^{-1} \circ g^{-1}$
- Let $|A| = m$, $|B| = n$. We want to count the number of functions from A to B
  1. all: n^m
  2. injection: $P(n, m) = n(n-1)\cdots(n-m+1)$ if $n \geq m$
  3. bijection: $\sum_{j=0}^{n}(-1)^j\binom{n}{j}(n-j)^m$ if $m \geq n$
- lg, log, ln
- $\lg^k n$, $\lg^{(k)} n$, $\lg^* n$

Functions III

- $\chi_S : U \to \{0, 1\}$ where $\chi_S(x) = 1$ iff $x \in S$ (characteristic function, indicator function)
  1. $\chi_{A\cap B} = \chi_A \chi_B$
  2. $\chi_{A\cup B} = \chi_A + \chi_B - \chi_A \chi_B$
  3. $\chi_{\overline{A}} = \mathbf{1} - \chi_A$
  4. $\chi_{A\triangle B} = \chi_A + \chi_B - 2\chi_A \chi_B$
  5. $\chi_{A\to B} = \mathbf{1} - \chi_A + \chi_A \chi_B$
  6. $\chi_{A\leftrightarrow B} = \mathbf{1} - \chi_A - \chi_B + 2\chi_A \chi_B$
  7. $\chi_A \chi_A = \chi_A$

Example

$$|A\cup B\cup C| = |A|+|B|+|C|-|A\cap B|-|A\cap C|-|B\cap C|+|A\cap B\cap C|$$

Binary Relations I

A subset R of $A \times B$ or $A \times A$.

- reflexivity: aRa
  symmetry: $aRb \implies bRa$
  asymmetry: $aRb \implies b \not R a$
  antisymmetry: aRb and $bRa \implies a = b$
  transitivity: aRb and $bRc \implies aRc$
- graph representation:
  $G = (V, E)$, $V = A$ and $(a, b) \in E$ iff aRb
- equivalence relation:
  1. reflexivity: $a \sim a$
  2. symmetry: $a \sim b \implies b \sim a$
  3. transitivity: $a \sim b$ and $b \sim c \implies a \sim c$
- equivalence class: $[a] := \{b \mid b \sim a\}$

Binary Relations II

- binary operator on equivalence classes:
  1. compatible: $a \circ b \sim c \circ d$ if $a \sim c$ and $b \sim d$ where $\circ$ is a binary operator
- closure: the closure of a relation R with respect to a property P
  the minimum relation S (if exists) that contains R and has property P

Example

- reflexive closure
- transitive closure

The following variables are all integers.

- $a|b$ (divisibility)
  There exists k such that $b = ak$.
- division theorem: Given integers a and $d \neq 0$. Then $a = dq + r$ where $0 \leq r < |d|$ has unique solution q and r.
  (a: dividend, d: divisor, q: quotient, r: remainder)
  $r = a \mod d$
- prime: A positive integer that has exact two positive divisors, i.e. 1 and itself.
- exactly divide: $p^k \parallel n$ iff $p^k|n$ but $p^{k+1} \not| n$
- congruence: $a \equiv b \pmod{n}$ iff $n|a-b$
- Euclidean Algorithm: $\gcd(a,b) = \gcd(b, a \mod d)$ if $b \neq 0$

Number Theory II

- Extended Euclidean Algorithm: Given n, a, and b. The equation $n = ax + by$ has integral solutions x and y iff $\gcd(a, b) | n$.
- $p | ab$ iff $p | a$ or $p | b$ where p is a prime

Proof.

($\Longrightarrow$) If $p \not| a$, then $\gcd(p, a) = 1$. Hence $1 = px + ay$ for some integers x and y. $\therefore b = bpx + aby \implies p | b$. □

- Euler's totient function: $\phi(m) = |\Phi(m)|$ where $\Phi(m) = \{a | \ 1 \le a \le m \text{ and } \gcd(a, m) = 1\}$
  $\phi(mn) = \phi(m)\phi(n)$ if $\gcd(m, n) = 1$ (multiplicative)
- $a^{p-1} \equiv 1 \pmod{p}$ (Fermat)
  $a^{\phi(m)} \equiv 1 \pmod{m}$ if $a \perp m$ (Euler)

Formal Language I

- alphabet Σ: any set of symbols
  $a \in \Sigma$: letter, character, symbol
- string over Σ: $x \in \Sigma^*$
  ϵ: the empty string
- language: any set of strings over Σ, i.e., $L \in 2^{\Sigma^*}$
  A language is finite iff $|L|$ is finite
- operations on strings: $x, y \in \Sigma^*$, $a \in \sigma$
  1. concatenation: xy
  2. reverse: $x^R := ay^R$ if $x = ya$; $\epsilon^R = \epsilon$
  3. repeat: $x^k := xx^{k-1}$ if $k \geq 1$; $x^0 := \epsilon$

Formal Language II

- operations on languages: $A, B \subseteq \Sigma^*$
  1. product: $AB := \{xy \mid x \in A \text{ and } y \in B\}$
  2. repeat: $A^k := \{x^k \mid x \in A\}$; $A^0 := \{\epsilon\}$
  3. union, intersection, etc
  4. Kleene's star: $A^* := \bigcup_{k \geq 0} A^k$
- membership problem (or recognition problem): to determine if $x \in L$ for language L.

Discrete Probability I

- sample space: Ω all possible outcomes of experiments
- event: any subset of Ω
- probability measure $P, \Pr$: a function from 2^{Ω} to $[0, 1]$ such that
  1. $\Pr(\Omega) = 1$
  2. $\Pr(\bigcup_{k=1}^{\infty} A_k) = \sum_{k=1}^{\infty} \Pr(A_k)$ where $A_i \cap A_j = \emptyset$ for $i \neq j$
- discrete random variable: a function $X : \Omega \to \mathbb{Z}$
- independent:
  1. on events:
     two events: $\Pr(A \cap B) = \Pr(A)\Pr(B)$;
     more than two events $A_1, A_2, \ldots, A_n$:
     $\Pr(A_{j_1} \cap A_{j_2} \cap \cdots \cap A_{j_k}) = \Pr(A_{j_1})\Pr(A_{j_2})\cdots\Pr(A_{j_k})$ for any indices $1 \leq j_1 \leq \cdots \leq j_k \leq n$ where $2 \leq k \leq n$

Discrete Probability II

2. on random variables:
   two r.v.'s X and Y:
   $\Pr(x \in X, y \in Y) = \Pr(x \in X)\Pr(y \in Y)$ for all $x, y \in \mathbb{Z}$
   more than two r.v.'s $X_1, X_2, \ldots, X_n$: for any intervals $B_1, B_2, \ldots, B_n$,
   $\Pr(X_1 \in B_1, \ldots, X_n \in B_n) = \Pr(X_1 \in B_1) \cdots \Pr(X_n \in B_n)$.

- expectation of an r.v. X: $E(X) = \sum_k k \Pr(X = k)$
  $E(X + Y) = E(X) + E(Y)$ for any r.v.'s X and Y;
  $E(XY) = E(Y)E(Y)$ when X and Y are independent
- generating function:
  1. probability generating function:
     $\phi(t) = E(t^X) = \sum_k \Pr(X = k)t^k$, defined for $|t| \leq 1$
  2. moment generating function: $\psi(t) = E(e^{tX})$
  3. characteristic function (Fourier transform): $\chi(t) = E(e^{itX})$

Calculus

- derivative: $\frac{dy}{dx} = f'(x)$ (Gottfried Leibnitz); $\dot{x}$ (Isaac Newton)
- integral: $\int f dx$ (Leibnitz); $\overset{|}{x}$ (Newton)
- chain rule: $\frac{dz}{dx} = \frac{dz}{dy}\frac{dy}{dx}$ where $y = f(x), z = g(y)$
- $\frac{d^2 f}{dx^2} = \ddot{y} = f''(x)$
- integration by substitution: $\int y dx = \int y \frac{dx}{du} du$

Numeral Systems I

▸ Wiki

- Roman numerals: I (1), V (5), X (10), L (50), C (100), D (500), M (1000), $\bar{V}$ (5000), ...

Useful Links

- Merriam-Webster Dictionary ▸ Link
- Wikipedia ▸ Link

Wikipedia

- typesetting of mathematical notation ▸ Wiki
- mathematical symbols ▸ Wiki
- ISO 31-11 ▸ Wiki

References I

K. H. Rosen (editor), Handbook of Discrete and Combinatorial Mathematics, CRC Press LLC, 2000.

Wikipedia, http://wikipedia.org/.