1. Speaking Mathematically

- variable: place holder for an object
- statement: sentence that is true or false, but not both

2. Logic of compound statements

- $p \to q \equiv \neg p \vee q$
- converse: $q \to p$
- inverse: $\neg p \to \neg q$
- order of operations for logical operators: 1) negations, 2) $\wedge, \vee$, 3) $\longrightarrow, \longleftrightarrow$
- sufficient condition: r is a sufficient condition for s means "if r then s"
- necessary condition: r is a necessary condition for s means "if not r then not s"
- r is a necessary and sufficient condition for s: "r if, and only if, s"

Valid Argument Forms

- modus ponens: $p \to q; p; q.$
- modus tollens: $p \to q; \neg q; p.$
- generalization: $p; p \vee q$ and mirror
- specialization: $p \wedge q; p.$ and mirror
- elimination: $p \vee q; \neg q; p.$ and mirror
- transitivity: $p \to q; q \to r; r.$

3. Logic of Quantified Statements

- Predicate: a sentence with finitely many variables that becomes a statement when each variable is concretely instantiated.
- Domain of a predicate variable (i.e. a variable in a predicate) is the set of all values it can hold
- Truth Set of $P(x)$ where x has domain D is $\{x \in D \mid P(x)\}$

4. Elementary Number Theory & Methods of Proof

4.1 to 4.3

for integers $n > 1$:

- n is prime $\Leftrightarrow \forall r, s \in \mathbb{Z}^+, n = rs \to (r = 1 \wedge s = n) \vee (r = n \wedge s = 1)$
- n is composite $\Leftrightarrow \exists r, s \in \mathbb{Z}^+$ s.t. $1 < r < n \wedge 1 < s < n \wedge rs = n$

Divisibility: (for $n, d \in \mathbb{Z}, d \neq 0$) $d \mid n \Leftrightarrow \exists k \in \mathbb{Z}, n = dk$

4.4 to 4.6

- Quotient-Remainder Theorem:$\forall n, d \in \mathbb{Z}, d \neq 0, \exists q, r \in \mathbb{Z}, n = dq + r \wedge 0 \leq r < d$
- triangle inequality: $\forall x, y \in \mathbb{R}, |x + y| \leq |x| + |y|$

5. Sequences & Induction

Basic Sequences

- Recursive Summation: $\sum_{k=m}^{n} a_k = \sum_{k=m}^{n-1} a_k + a_n$
- n choose r: $\binom{n}{r} = \frac{n!}{r!(n-r)!}$
- $\sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}$ (sum of geometric sequence)
- Closed form for a sum with a variable number of terms is a formula that contains neither an ellipsis nor summation notation

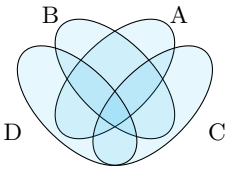
Induction

1. induction: To prove statements like "for all integers $n \geq a$, property $P(n)$ is true", perfom two steps: 1) Show that $P(a)$ is true and 2) Show that if $k \geq a$ and $P(k)$ then $P(k+1)$:
2. strong induction: like mathematical inductions but with several base cases (show that $P(a), P(a+1), P(a+2)$)
3. well-ordering principle: Let $S \subseteq Z$ be a nonempty set of integers where $\exists x \in \mathbb{Z}$ s.t. $\forall s \in S, s > x$. Then S has a least element.
4. catalan numbers: $C_n = \frac{1}{n+1}\binom{2n}{n}$ (how many ways are there to parenthesize n multiplications i.e. a propduct of $n+1$ numbers)

6. Set Theory

Venn diagram for 4 sets

Note: n sets have 2^n regions ($2^n - 1$ inside + outside)



Basic Definitions

- Subset: $A \subseteq B \Leftrightarrow \forall x \in A, x \in B$
- Not Subset: $A \not\subseteq B \Leftrightarrow \exists x \in A$ s.t. $x \notin B$
- Proper Subset: $A \subsetneq B \Leftrightarrow A \subseteq B \wedge B \not\subseteq A$
- Set Equality: $A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$

Set Operations

- Union: $x \in X \cup Y \Leftrightarrow x \in X \vee x \in Y$
- Intersection: $x \in X \cap Y \Leftrightarrow x \in X \wedge x \in Y$
- Difference: $x \in X - Y \Leftrightarrow x \in X \wedge x \notin Y$
- Complement: $x \in X^c \Leftrightarrow x \notin X$
- Cartesian Product: $(x, y) \in X \times Y \Leftrightarrow x \in X \wedge y \in Y$

Interval Notation

- $(a, b) = x \in \mathbb{R} : a < x < b$
- $[a, b) = x \in \mathbb{R} : a \leq x < b$
- $(a, b] = x \in \mathbb{R} : a < x \leq b$
- $[a, b] = x \in \mathbb{R} : a \leq x \leq b$
- $(a, \infty) = x \in \mathbb{R} : x > a$
- $[a, \infty) = x \in \mathbb{R} : x \geq a$
- $(-\infty, b) = x \in \mathbb{R} : x < b$
- $(-\infty, b] = x \in \mathbb{R} : x \leq b$

Special Concepts

- Disjoint Sets: $A \cap B = \emptyset$
- Partition: Sets $A_1, A_2, ...$ where: 1) union is total set and 2) $A_1, A_2, ...$ are mutually disjoint
- Power Set: $\mathscr{P}(A)$ = set of all subsets

Boolean Algebra Laws

note: $0 = F = \phi, 1 = T = U, + = \vee = \cup, \cdot = \wedge = \cap, \overline{x} = \neg x = A^c$

- Closure: $\forall a, b \in B, a+b \in B$ and $a \cdot b \in B$
- Commutativity: $\forall a, b \in B, a + b = b + a$ and $a \cdot b = b \cdot a$
- Associativity: $\forall a, b, c \in B, (a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- Distributivity: $\forall a, b, c \in B, a + (b \cdot c) = (a+b) \cdot (a+c)$ and $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$
- Identity: $\exists 0, 1 \in B$, s.t. $a + 0 = a$ and $a \cdot 1 = a$
- Complement: $\forall a \in B, \exists \overline{a} \in B$, s.t. $a + \overline{a} = 1$ and $a \cdot \overline{a} = 0$
- Uniqueness of the Complement Law: $\forall a, x \in B$, if $a + x = 1$ and $a \cdot x = 0$ then $x = \overline{a}$
- Uniqueness of 0 and 1: If there exists $x \in B$ such that $\forall a \in B, a + x = 1$ and $a \cdot x = 0$ then $x = \overline{a}$
- Double Complement Law: $\forall a \in B, \overline{(\overline{a})} = a.$
- Idempotent Law: $a + a = a$ and $a \cdot a = a$
- Universal Bound Law: $a + 1 = 1$ and $a \cdot 0 = 0$
- De Morgan's Laws: $\overline{a + b} = \overline{a} \cdot \overline{b}$ and $\overline{a \cdot b} = \overline{a} + \overline{b}$
- Absorption Laws: $(a + b) \cdot a = a$ and $(a \cdot b) + a = a$
- Complements of 0 and 1: $\overline{0} = 1$ and $\overline{1} = 0.$

Russell's Paradox

(e.g. barber who shaves all people who don't shave themselves)

- $S = \{A : A \text{ is a set}, A \notin A\}$
- If $S \in S$ then $S \notin S$
- If $S \notin S$ then $S \in S$
- Resolution: Sets defined within *known* domain

7. Functions

Basic Definitions

- Function $f : X \to Y$
- Total: Every input has output
- Single-valued: One output per input
- Domain: Input set X
- Codomain: Output set Y
- Range: $f(X) = \{f(x) : x \in X\}$

Special Functions

- Identity: $I_X : X \to X$ where $I_X(a) = a$ for all $a \in X$
- Image of a set A: $f(A) = \{f(x) : x \in A\}$
- Preimage: $f^{-1}(y) = \{x : f(x) = y\}$
- Preimage of set: $f^{-1}(A) = \{x \in X : f(x) \in A\}$

Function Properties

- Injective (1-1): $f(x) = f(y) \Leftrightarrow x = y$
- Surjective (onto): $\forall y \in Y, \exists x : f(x) = y$
- Bijective: Both injective and surjective
- If a function is bijective (is a bijection), then its inverse is also a function (as opposed to a general relation).

Logarithm Properties

- $\log_b(xy) = \log_b(x) + \log_b(y)$
- $\log_b(\frac{x}{y}) = \log_b(x) - \log_b(y)$
- $\log_b(x^y) = y \log_b(x)$
- $\log_c(x) = \frac{\log_b(x)}{\log_b(c)}$

Algorithm Correctness

Basic Concepts

- **Pre-condition:** Predicate over input values describing valid initial states
- **Post-condition:** Predicate over output values describing required final states
- Algorithm is correct if true pre-condition implies true post-condition

Loop Properties

- Loop is correct iff:
  - Pre-condition satisfied
  - Loop terminates in finite steps
  - Post-condition satisfied
- **Loop Invariant:** is a predicate whose domain consists of integers with the following property: if the predicate is true at before an iteration, then it is true after the iteration as well. If the following additional properties hold, then the loop is correct with respect to its pre- and post-conditions:
  - predicate is true before 1st iteration
  - if the loop terminates after a finite number of iterations, then the truth of the invariant ensures the truth of the post-condition

Loop Invariant Theorem

Given a while-loop with guard G along with its pre- and post-conditions and its loop invariant I(n). If all of the following are true, then the loop is correct with respect to its pre- and post-conditions.

1. **Basis property:** pre-condition ensures that $I(0)$ is true.
2. **Inductive Property:** for all integers $k \geq 0$, if the guard G and loop invariant $I(k)$ are both true at the start of an iteration, then $I(k+1)$ is true at the end of the iteration.
3. **Eventual Falsity of Guard:** G becomes false in finite steps
4. **Post-condition:** If N is the least number of iterations after which the guard G is false and the loop invariant $I(N)$ is treu, then the post-condition is true.