21-127 Final Exam Study Guide

Mary Radcliffe

1 Exam Structure

Your final exam will have 10 problems, though some will have multiple parts. The exam will have the following structure.

- The first 3 questions will deal with material covered since the second exam. Specifically: relations, equivalence relations, modular arithmetic and related issues, posets. The remaining 7 questions will be cumulative, and may include concepts covered since the second exam.
- You should expect questions that either ask you to directly state or explain key theorems from the semester. You should expect questions that either ask you to directly define terms or give examples of objects illustrating key definitions/concepts.
- You should expect some short answer questions, in which you will be asked to write a brief response in words explaining a concept (rather than writing a proof)
- The difficulty level of the proofs on the final should be similar to the difficulty level of midterm proofs.

2 Major Topics

2.1 Propositional Logic and Proof Techniques

1. Understanding propositional formulae: propositional variables, conjunction, disjunction, negation, conditional
2. De Morgan's Laws
3. Quantifiers, ordering of quantifiers, negations
4. Direct Proof: proving statements of the form $p \Rightarrow q$ by assuming p and deriving q.
5. Biconditional: proving statements of the form $p \Leftrightarrow q$.
6. Proof by contradiction: proving statements of the form $p \Rightarrow q$ by assuming p and $\neg q$ and deriving a contradiction.
7. Proof by cases: proving statements of the form $p \vee q \Rightarrow r$ by taking two cases: $p \Rightarrow r$ and $q \Rightarrow r$.
8. Proof by contrapositive: proving statements of the form $p \Rightarrow q$ by assuming $\neg q$ and deriving $\neg p$.
9. Law of Excluded Middle
10. Induction: weak and strong

2.2 Set Theory and functions

1. Basic definitions, set builder notation
2. Unions, intersections, complements, power sets, Cartesian products
3. Proving equality between sets using double containment
4. De Morgan's Laws
5. Basic definitions for functions: domain, codomain, graph, injective, surjective, bijective, image, preimage, compositions, left/right/two-sided inverses
6. Well-definedness: definitions, how to prove

2.3 Counting: finite

1. Definition of finiteness
2. Basic counting theorems: Products, unions, intersections
3. Inclusion-Exclusion
4. Permutations and binomial coefficients, Binomial Theorem
5. Counting in 2 ways
6. Counting by bijection

2.4 Counting: infinite

1. Definition of two sets having the same size
2. Definition of countably infinite, uncountably infinite
3. Proof that the finite product of countable sets is countable
4. Proof that the countable union of countable sets is countable
5. Proof that $\mathbb{Q}$ is countable
6. Cantor's Diagonalization and proofs of uncountability

2.5 Equivalence Relations

1. Basic definitions of relations, equivalence relations
2. Understanding of equivalence relations via partition of ground set

2.6 Divisibility and Number Theory

1. Division Theorem
2. GCDs: basic definitions and theorems
3. Euclidean Algorithm
4. Bezout's Lemma
5. Primes: basic definitions
6. Fundamental Theorem of Arithmetic

2.7 Modular arithmetic

1. Basic definitions of congruence
2. Understanding of modular equivalence as an equivalence relation, and $\mathbb{Z}_n$
3. Arithmetic: how to perform basic operations
4. Multiplicative inverses: when they exist, and how to find them
5. Fermat's Little Theorem, Euler's Totient Theorem
6. Chinese Remainder Theorem

2.8 Posets

1. Basic definitions of poset as a relation
2. Key terminology: minimum, maximum, supremum (aka LUB, aka join), infimum (aka GLB, aka meet), lattice
3. Understanding of Hasse diagram for representing poset structure

3 Theorems with Names

You should be able to state/explain anything on this list when referred to by name.

- De Morgan's Laws for Propositions
- De Morgan's Laws for Quantifiers
- Pigeonhole Principle
- Principle of Weak Induction
- Principle of Strong Induction
- Fundamental Theorem of Arithmetic
- De Morgan's Laws for Sets
- Well-Ordering Principle
- Pascal's Identity
- Binomial Theorem
- Principle of Includsion/Exclusion
- Cantor's Diagonalization
- Division Theorem
- Euclidean Algorithm
- Bézout's Lemma
- Euler's Totient Theorem
- Freshman Exponentiation Theorem
- Fermat's Little Theorem
- Chinese Remainder Theorem

4 Terms and Notation

- Proposition
- Conjunction ($\wedge$)
- Disjunction ($\vee$)
- Exclusive disjunction ($\dot{\vee}$)
- Negation ($\neg$)
- Propositional formula
- Logical equivalence ($\equiv$)
- Tautology
- Conditional operator ($\Rightarrow$)
- Biconditional operator ($\Leftrightarrow$)
- Universal quantifier ($\forall$)
- Existential quantifier ($\exists$)
- Unique existential quantifier ($\exists!$)
- Rational number ($\mathbb{Q}$)
- Irrational number ($\mathbb{R}\backslash\mathbb{Q}$)
- Limit
- Peano axioms (and associated terms)
- Formal definitions for $\sum_{k=m}^{n} a_k$, $\prod_{k=m}^{n} a_k$
- Set
- Set-Builder notation ($\{x \in \Omega \mid p(x)\}$)
- Empty set ($\emptyset$)
- Subset ($\subseteq$)
- Superset ($\supseteq$)
- Power set ($\mathcal{P}(X)$)
- Intersection ($\cap$)'
- Disjoint/pairwise disjoint
- Union ($\cup$)
- Cartesian product ($\times$)
- (Universal) complement (X^c)
- Relative complement ($X\backslash Y$)
- Formal definitions for $\bigcup_{k=m}^{n} A_k$, $\bigcap_{k=m}^{n} A_k$
- Lower bound
- Upper bound
- Infimum in $\mathbb{R}$ ($\inf(S)$)
- Supremum in $\mathbb{R}$ ($\sup(S)$)
- Minimum in $\mathbb{R}$ ($\min(S)$)
- Maximum in $\mathbb{R}$ ($\max(S)$)
- Well-ordered
- Function
- Domain
- Codomain
- Well-defined (totality, existence, uniqueness)
- Identity function (ι_X)
- Identically equal functions
- Image ($f(A)$)
- Range ($f(X)$)
- Restriction ($f|_U$)
- Preimage ($f^{-1}(V)$)
- Composition ($f \circ g$)
- Injective/injection
- Surjective/surjection
- Bijective/bijection
- Left inverse
- Right inverse
- (Two-sided) inverse, invertible (f^{-1})
- Finite
- Infinite
- Cardinality ($|X|$)
- Permutation
- Permutation of n (S_n)
- Binomial coefficient ($\binom{n}{k}$)
- Pairwise disjoint (finite) partition
- Countably infinite
- Uncountably infinite
- Countable
- Divides/divisible ($a|b$)
- Divisor/factor
- Multiple
- Quotient
- Remainder
- Greatest common divisor (gcd)
- Least common multiple (lcm)
- Coprime/relatively prime ($\perp$)
- Relation from X to Y
- Relation on X
- Reflexive relation
- Symmetric relation
- Transitive relation
- Antisymmetric relation
- Equivalence relation
- Equivalence class ($[x]_\sim$)
- Congruent modulo n ($a \equiv b \pmod{n}$)
- Integers modulo n ($\mathbb{Z}_n$)
- Multiplicative inverse modulo n
- Order, finite order
- Euler's Totient function (φ)
- Poset
- Lower bound in a poset
- Upper bound in a poset
- Infimum/Meet in a poset ($\wedge$)
- Supremum/Join in a poset ($\vee$)
- Hasse diagram
- Minimum in a poset ($\perp$)
- Maximum in a poset ($\top$)