Discrete Mathematics
CST Part IA Paper 2

Victor Zhao
xz398@cam.ac.uk

1 Proof

1. Some mathematical jargon:
   - **Statement**: A sentence that is either true or false — but not both.
   - **Predicate**: A statement whose truth depends on the value of one or more variables.
   - **Theorem**: A very important true statement.
   - **Proposition**: A less important but nonetheless interesting true statement.
   - **Lemma**: A true statement used in proving other true statements.
   - **Corollary**: A true statement that is a simple deduction from a theorem or proposition.
   - **Conjecture**: A statement believed to be true, but for which we have no proof.
   - **Proof**: Logical explanation of why a statement is true; a method for establishing truth.
   - **Logic**: The study of methods and principles used to distinguish good (correct) from bad (incorrect) reasoning.
   - **Axiom**: A basic assumption about a mathematical situation. Axioms can be considered facts that do not need to be proved (just to get us going in a subject) or they can be used in definitions.
   - **Definition**: An explanation of the mathematical meaning of a word (or phrase). The word (or phrase) is generally defined in terms of properties.
   - A statement is *simple* (or *atomic*) when it cannot be broken into other statements, and it is *composite* when it is built by using several (simple or composite statements) connected by logical expressions
2. Contraposition:
   The contrapositive of $P \implies Q$ is $\neg Q \implies \neg P$.
3. Modus Ponens: If P and $P \implies Q$ holds then so does Q.

$$\frac{P \qquad P \implies Q}{Q}$$

4. Some notations:
   - Implication: $\implies$
   - Bi-implication: $\iff$
   - Universal quantification: $\forall x.P(x)$
   - Existential quantification: $\exists x.P(x)$
   - Unique existence: $\exists! x.P(x)$

$$\exists! x.P(x) \iff \exists x.P(x) \land \Big(\forall y.\forall z.\big(P(y) \land P(z)\big) \implies y = z\Big)$$

   - Conjunction: $\land$
   - Disjunction: $\lor$
   - Negation: $\neg$
5. Equality axioms:
   - Every individual is equal to itself.

$$\forall x. x = x$$

   - (Leibniz equality) For any pair of equal individuals, if a property holds for one of them, then ait also holds for the other one.

$$\forall x.\, \forall y.\, x = y \implies (P(x) \implies P(y))$$

2 Numbers

1. Definitions of real numbers. A real number is:
   - **rational** if it is of the form $\frac{m}{n}$ for a pair of integers m and n; otherwise it is **irrational**;
   - **positive** if it is greater than 0, and **negative** if it is smaller than 0;
   - **nonnegative** if it is greater than or equal to 0, and **nonpositive** if it is smaller than or equal to 0;
   - **natural** if it is a nonnegative integer.
2. Additive structure $(\mathbb{N}, 0, +)$ of natural numbers with zero and addition is a commutative monoid (a *monoid* is a semigroup with an identity element; a *semigroup* preserves closure and associativity):
   - Monoid laws:
   $$0 + n = n + 0 = n \quad \text{(identity)}$$
   $$(l + m) + n = l + (m + n) \quad \text{(associativity)}$$
   - Commutativity law:
   $$m + n = n + m$$
3. Multiplicative structure $(\mathbb{N}, 1, \cdot)$ of natural numbers with one and multiplication is a commutative monoid:
   - Monoid laws:
   $$1 \cdot n = n \cdot 1 = n$$
   $$(l \cdot m) \cdot n = l \cdot (m \cdot n)$$
   - Commutativity law:
   $$m \cdot n = n \cdot m$$
4. The overall structure $(\mathbb{N}, 0, +, 1, \cdot)$ is a commutative semiring:
   - $(\mathbb{N}, 0, +)$ is a commutative monoid;
   - $(\mathbb{N}, 1, \cdot)$ is a monoid;
   - Multiplication is distributive over addition:
   $$l \cdot (m + n) = l \cdot m + l \cdot n$$
   - Multiplication by 0 annihilates $\mathbb{N}$:
   $$0 \cdot n = n \cdot 0 = 0$$
5. Cancellation:
   - Additive cancellation: for all natural numbers k, m, n,
   $$k + m = k + n \implies m = n$$
   - Multiplicative cancellation: for all natural numbers k, m, n,
   $$\text{if } k \neq 0 \text{ then } k \cdot m = k \cdot n \implies m = n$$
6. Inverses:
   - A number x is said to admit an **additive inverse** whenever there exists a number y such that $x + y = 0$;
   - A number x is said to admit an **multiplicative inverse** whenever there exists a number y such that $x \cdot y = 1$.
7. The integers $\mathbb{Z}$ form a commutative ring, and the rationals $\mathbb{Q}$ form a field:
   - A *group* is a monoid in which every element has an inverse;
   - A *ring* is a semiring $(0, +)$, $(1, \cdot)$ where $(0, +)$ is a commutative group. It is commutative if $(1, \cdot)$ is also commutative;
   - A *field* is a ring where every non-zero element has a multiplicative inverse.

8. Divisibility and congruence:
   - Let d and n be integers. We say that d *devides* n, and write $d|n$, whenever there exists an integer k such that $n = k \cdot d$;
   - Fix a positive integer m. For integers a and b, we say that *a is congruent to b modulo m*, and write $a \equiv b \pmod{m}$, whenever $m|(a-b)$.
9. For all prime numbers p and integers $0 \leq m \leq p$, either $\binom{p}{m} \equiv 0 \pmod{p}$ or $\binom{p}{m} \equiv 1 \pmod{p}$.
   For $0 < m < p$, $p|\binom{p}{m}$ and $(p-m)|\binom{p-1}{m}$.
10. The Freshman's Dream: For all natural numbers m, n and primes p,
    $$(m+n)^p \equiv m^p + n^p \pmod{p}$$
11. The Dropout Lemma: For all natural numbers m and primes p,
    $$(m+1)^p \equiv m^p + 1 \pmod{p}$$
12. The Many Dropout Lemma: For all natural numbers m and i, and primes p,
    $$(m+i)^p \equiv m^p + i \pmod{p}$$
13. Fermat's Little Theorem: For all natural numbers i and primes p,
    - $i^p \equiv i \pmod{p}$, and
    - $i^{p-1} \equiv 1 \pmod{p}$ whenever i is not a multiple of p.
14. The Division Theorem: For every natural number m and positive natural number n, there exists a unique pair of integers q and r such that $q \geq 0$, $0 \leq r \leq n$, and $m = q \cdot n + r$.
15. Modular arithmetic: For all natural numbers $m > 1$, the modular-arithmetic structure
    $$(\mathbb{Z}_m, 0, +_m, 1, \cdot_m)$$
    is a commutative ring.
    For prime p, $\mathbb{Z}_p$ is a field.
16. Greatest Common Divisor: For all positive integers m and n,
    $$\gcd(m,n) = \begin{cases} n & \text{, if } n|m \\ \gcd\big(n, \mathrm{rem}(m,n)\big) & \text{, otherwise} \end{cases}$$
17. Some fundamental properties of gcds:
    - Commutativity: $\gcd(m,n) = \gcd(n,m)$,
    - Associativity: $\gcd\big(l, \gcd(m,n)\big) = \gcd\big(\gcd(l,m), n\big)$,
    - Distributivity: $\gcd(l \cdot m, l \cdot n) = l \cdot \gcd(m,n)$.
18. Theorem: For positive integers k, m, and n, if $k|(m \cdot n)$ and $\gcd(k,m) = 1$ then $k|n$.
    Corollary (Euclid's Theorem): For positive integers m, n, and prime p, if $p|(m \cdot n)$ then $p|m$ or $p|n$.
19. For all positive integers m and n,
    - $n \cdot \mathrm{lc}_2(m,n) \equiv \gcd(m,n) \pmod{m}$, and
    - whenever $\gcd(m,n) = 1$,
      $[\mathrm{lc}_2(m,n)]_m$ is the multiplicative inverse of $[n]_m$ in $\mathbb{Z}_m$.

20. Principle of Induction:
Let $P(m)$ be a statement for m ranging over the natural numbers greater than or equal to a fixed natural number l. If
    - $P(l)$ holds, and
    - $\forall n \geq l$ in $\mathbb{N}.\big(P(n) \implies P(n+1)\big)$ also holds,

    then
    - $\forall m \geq l$ in $\mathbb{N}.P(m)$ holds.
21. Principle of Strong Induction:
Let $P(m)$ be a statement for m ranging over the natural numbers greater than or equal to a fixed natural number l. If
    - $P(l)$ holds, and
    - $\forall n \geq l$ in $\mathbb{N}.\Big(\big(\forall k \in [l..n].P(k)\big) \implies P(n+1)\Big)$ also holds,

    then
    - $\forall m \geq l$ in $\mathbb{N}.P(m)$ holds.
22. Well-Founded Induction:
Definition: a *well-founded relation* is a binary relation $\prec$ on a set A such that there are no infinite descending chains $\cdots \prec a_i \prec \cdots \prec a_1 \prec a_0$. When $a \prec b$ we say a is a *predecessor* of b.
Principle of Well-Founded Induction: Let $\prec$ be a well-founded relation on a set A. if
    - $\forall a \in A.\Big(\big(\forall b \prec a.P(b)\big) \implies P(a)\Big)$ holds,

    then
    - $\forall a \in A.P(a)$ holds.
23. Fundamental Theorem of Arithmetic: For every positive integer n there is a unique finite ordered sequence of primes $(p_1 \leq \cdots \leq p_l)$ with $l \in \mathbb{N}$ such that
$$n = \prod_{i=1}^{l} p_i.$$

3 Sets

1. Axioms:
   - Extensionality axiom: Two sets are equal if they have the same elements.
   $$\forall \text{ sets } A, B \,.\, A = B \iff (\forall x . x \in A \iff x \in B)$$
   - Powerset axiom: For any set, there is a set consisting of all its subsets.
   - Pairing axiom: For every a and b, there is a set with a and b as its only elements.
   - Union axiom: Every collection of sets has a union.
   - Infinity axiom: There is an infinite set, containing $\emptyset$ and closed under successor. $(\mathrm{Succ}(x) =_{\mathrm{def}} x \cup \{x\})$
   - Axiom of choice: Every surjection has a section (right inverse).
   - Replacement axiom: The direct image of every definable functional property on a set is a set.
2. Cardinality:
   - $\forall$ finite set $U . \#\mathcal{P}(U) = 2^{\#U}$
   - $\forall$ sets $A, B . \#(A \times B) = \#A \times \#B$
   - $\forall$ sets $A, B . \#(A \uplus B) = \#A + \#B$
3. Subsets:
   $$A \subseteq B \iff (\forall x . x \in A \implies x \in B)$$
   $$A \subset B \iff (A \subseteq B \land A \neq B)$$
   Reflexivity: $\forall$ set $A \,.\, A \subseteq A$
   Transitivity: $\forall$ set $A, B, C \,.\, (A \subseteq B \land B \subseteq C) \implies A \subseteq C$
   Antisymmetry: $\forall$ set $A, B \,.\, (A \subseteq B \land B \subseteq A) \implies A = B$
4. Separation principle: For any set A and any definable property P, there is a set containing precisely those elements of A for which the property P holds.
   $$\{x \in A \mid P(x)\}$$
5. The powerset Boolean algebra: $\left(\mathcal{P}(U), \emptyset, U, \cup, \cap, (\cdot)^c\right)$
   - For all $A, B \in \mathcal{P}(U)$,
   $$A \cup B = \{x \in U \mid x \in A \lor x \in B\} \in \mathcal{P}(U)$$
   $$A \cap B = \{x \in U \mid x \in A \land x \in B\} \in \mathcal{P}(U)$$
   $$A^c = \{x \in U \mid \neg(x \in A)\} \in \mathcal{P}(U)$$
   - The union operateion $\cup$ and the intersection operation $\cap$ are associative, commutative, and idempotent:
   $$(A \cup B) \cup C = A \cup (B \cup C),\ A \cup B = B \cup A,\ A \cup A = A$$
   $$(A \cap B) \cap C = A \cap (B \cap C),\ A \cap B = B \cap A,\ A \cap A = A$$
   - The *empty set* $\emptyset$ is a neutral element for $\cup$ and the *universal set* U is a neutral element for $\cap$:
   $$\emptyset \cup A = U \cap A = A$$
   - The empty set $\emptyset$ is an annihilator for $\cap$ and the universal set U is an annihilator for $\cup$:
   $$\emptyset \cap A = \emptyset$$
   $$U \cup A = U$$
   - With respect to each other, the union operation $\cup$ and the intersection operation $\cap$ are distributive and absorptive:
   $$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
   $$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
   $$A \cup (A \cap B) = A \cap (A \cup B) = A$$

- The complement operation $(\cdot)^c$ satisfies complementation laws:

$$A \cup A^c = U, \ A \cap A^c = \emptyset$$

6. Ordered pair: $\langle a, b \rangle =_{\text{def}} \big\{\{a\}, \{a, b\}\big\}$
   Fundamental property or ordered pairing:

$$\forall a, b, x, y \ . \ \langle a, b \rangle = \langle x, y \rangle \Longleftrightarrow (a = x \wedge b = y)$$

7. Big Unions: Let U be a set. For a collection of sets $\mathcal{F} \in \mathcal{P}(\mathcal{P}(U))$ (i.e. $\mathcal{F} \subseteq \mathcal{P}(U)$),

$$\bigcup \mathcal{F} =_{\text{def}} \{x \in U \mid \exists A \in \mathcal{F}. x \in A\} \in \mathcal{P}(U)$$

   Idea:

$$\bigcup \{A_1, A_2, \cdots\} = (A_1 \cup A_2 \cup \cdots) \subseteq U$$

8. Big Intersections: Let U be a set. For a collection of sets $\mathcal{F} \in \mathcal{P}(\mathcal{P}(U))$ (i.e. $\mathcal{F} \subseteq \mathcal{P}(U)$),

$$\bigcap \mathcal{F} =_{\text{def}} \{x \in U \mid \forall A \in \mathcal{F}. x \in A\} \in \mathcal{P}(U)$$

   Idea:

$$\bigcap \{A_1, A_2, \cdots\} = (A_1 \cap A_2 \cap \cdots) \subseteq U$$

9. Tagging: $\{l\} \times A$
10. Disjoint Unions: $A \uplus B =_{\text{def}} \big(\{1\} \times A\big) \cup \big(\{2\} \times B\big)$

$$\forall x. x \in (A \uplus B) \Longleftrightarrow \big(\exists a \in A. x = (1, a)\big) \vee \big(\exists b \in B. x = (2, b)\big)$$

4 Relations

1. Some notations and definitions:
   - Relation: $\nrightarrow$
     For all finite sets A and B, $\#\text{Rel}(A, B) = 2^{\#A \cdot \#B}$
   - Partial function: $\rightharpoonup$
     Set of partial functions: $\rightleftharpoons$
     Every partial function $f : A \rightharpoonup B$ satisfies that: for each element a of A there is at most one element b of B such that $a \ f \ b$.

     $$\forall f \in \text{Rel}(A, B).\ f \in (A \rightleftharpoons B) \iff \forall a \in A. \forall b_1, b_2 \in B.\ a \ f \ b_1 \land a \ f \ b_2 \implies b_1 = b_2$$

     For all finite sets A and B, $\#(A \rightleftharpoons B) = (\#B + 1)^{\#A}$
   - Mapping: $\mapsto$
   - Function: $\rightarrow$
     Set of functions: $\Rightarrow$
     A partial function is total if its domain of definition coincides with its source.

     $$\forall f \in (A \rightleftharpoons B).\ f \in (A \Rightarrow B) \iff \forall a \in A.\ \exists b \in B.\ a \ f \ b$$

     $$\forall f \in \text{Rel}(A, B).\ f \in (A \Rightarrow B) \iff \forall a \in A.\ \exists! b \in B.\ a \ f \ b$$

     For all finite sets A and B, $\#(A \Rightarrow B) = \#B^{\#A}$
   - Injection: $\rightarrowtail$
     A function $f : A \rightarrow B$ is injective whenever

     $$\forall a_1,\ a_2 \in A.\ f(a_1) = f(a_2) \implies a_1 = a_2$$

   - Surjection: $\twoheadrightarrow$
     A function $f : A \rightarrow B$ is surjective whenever

     $$\forall b \in B.\ \exists a \in A.\ f(a) = b$$

     For all finite sets A and B, $\#\text{Sur}(A, B) =$
   - Bijection: A function $f : A \rightarrow B$ is bijective whenever there exists a (necessarily unique) function $g : B \rightarrow A$ (referred to as the inverse of f) such that

     $$g \circ f = \text{id}_A \quad \text{and} \quad f \circ g = \text{id}_B$$

     For all finite sets A and B,

     $$\#\text{Bij}(A, B) = \begin{cases} 0 & \text{, if } \#A \neq \#B \\ n! & \text{, if } \#A = \#B = n \end{cases}$$

2. Composition:
   Composition of two relations $R : A \nrightarrow B$ and $S : B \nrightarrow C$:

   $$S \circ R : A \nrightarrow C$$

   Relational composition is associative and has the identity relation as neutral element:

   $$\forall R : A \nrightarrow B,\ S : B \nrightarrow C,\ T : C \nrightarrow D\ .\ (T \circ S) \circ R = T \circ (S \circ R)$$

   $$\forall R : A \nrightarrow B\ .\ R \circ \text{id}_A = \text{id}_B \circ R = R$$

   $R^{\circ n}$: R composed with itself n times.
   $R^{\circ *} = \bigcup_{n \in \mathbb{N}} R^{\circ n}$

3. Preorders:
   A preorder $(P, \sqsubseteq)$ consists of a set P and a relation $\sqsubseteq$ on P satisfying the following two axioms:
   - Reflexivity: $\forall x \in P . x \sqsubseteq x$
   - Transitivity: $\forall x, y, z \in P . (x \sqsubseteq y \land y \sqsubseteq z) \implies x \sqsubseteq z$

   $R^{\circ *}$ is the reflexive-transitive closure of R
   $R^{\circ *}$ is the least preorder containing R
   $R^{\circ *}$ is the preorder freely generated by R

4. Isomorphism: $\cong$
   Two sets A and B are isomorphic (and have the same cardinality) whenever there is a bijection between them,

5. Equivalence relations:
   A relation E on a set A is an equivalence relation whenever it is:
   - Reflexive: $\forall x \in A.\ x\ E\ x$
   - Symmetric: $\forall x, y \in A.\ x\ E\ y \implies y\ E\ x$
   - Transitive: $\forall x, y, z \in A.\ (x\ E\ y \land y\ E\ z) \implies x\ E\ z$

6. Set partitions:
   A partition P of a set A is a set of non-empty subsets of A (that is, $P \subseteq \mathcal{P}(A)$ and $\emptyset \notin P$), whose elements are typically referred to as blocks, such that
   - The union of all blocks yields A: $\bigcup P = A$, and
   - All blocks are pairwise disjoint: $\forall B_1, B_2 \in P.\ B_1 \neq B_2 \implies B_1 \cap B_2 = \emptyset$

   For every set A: $\mathrm{EqRel}(A) \cong \mathrm{Part}(A)$

7. Enumerability:
   A set A is enumerable whenever there exists a surjection ($\mathbb{N} \twoheadrightarrow A$), or a injection ($A \rightarrowtail \mathbb{N}$), referred to as an enumeration.
   A countable set is one that is either empty or enumerable.

8. Relational images and functional images:
   Let $R : A \nrightarrow B$ be a relation.
   - The direct image of $X \subseteq A$ under R is the set $\overrightarrow{R}(X) \subseteq B$:

     $$\overrightarrow{R}(X) = \{b \in B | \exists x \in X\ .\ x\ R\ b\}$$

     This construction yields a function $\overrightarrow{R} : \mathcal{P}(A) \to \mathcal{P}(B)$.
   - The inverse image of $Y \subseteq B$ under R is the set $\overleftarrow{R}(X) \subseteq A$:

     $$\overleftarrow{R}(Y) = \{a \in A | \forall b \in B\ .\ a\ R\ b \implies b \in Y\}$$

     This construction yields a function $\overleftarrow{R}(Y) : \mathcal{P}(B) \to \mathcal{P}(A)$.

   Let $f : A \to B$ be a function.
   - For all $X \subseteq A$, $\overrightarrow{f}(X) = \{b \in B | \exists a \in X\ .\ f(a) = b\}$;
   - For all $Y \subseteq B$, $\overleftarrow{f}(Y) = \{a \in A | f(a) \in Y\}$.