Reference Sheet for CO142.1 Discrete Mathematics I

Autumn 2016

Proofs in Discrete Mathematics

1. Use Venn diagrams, directed graphs, or another visual representation to gain an intuition of what needs to be shown.
2. Use definitions to create a logical statement.
3. Use logical arguments to prove the statement.
   (a) In general, equivalences from CO140 should be sufficient.
   (b) If something is false, try to find a simple counterexample.
   (c) If under a for-all quantifier, consider an arbitrary object.
   (d) For an if-then statement, assume the antecedent and prove the consequent.
   (e) For an equality or if-and-only-if, ensure your argument is bidirectional.
4. Use definitions to return to set notation.

1 Sets

A *set* is a collection of definite and separate objects.

Russel's Paradox The collection $R \triangleq \{X \text{ is a set} | X \notin X\}$ is not a set. Can be proven by contradiction when considering a set R (consider the cases $R \in R$ and $R \notin R$).

Comparing Sets

1. *Subset*: $A \subseteq B \triangleq \forall x \in A\,(x \in B)$.
2. *Equality*: $A = B \triangleq A \subseteq B \wedge B \subseteq A$.

If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Basic Operators

1. Union: $A \cup B \triangleq \{x | x \in A \vee x \in B\}$.
2. Intersection: $A \cap B \triangleq \{x | x \in A \wedge x \in B\}$.
3. Difference: $A \backslash B \triangleq \{x | x \in A \wedge x \notin B\}$.
4. Symmetric Difference: $A \triangle B \triangleq (A \backslash B) \cup (B \backslash A)$.

A, B are *disjoint* $\triangleq A \cap B = \emptyset$.
To make any union $A \cup B$ disjoint, consider $A \cup (B \backslash A)$.

Properties of Basic Operators

1. *Idempotence*
   (a) $A \cup A = A$
   (b) $A \cap A = A$
2. *Commutativity*
   (a) $A \cup B = B \cup A$
   (b) $A \cap B = B \cap A$
   (c) $A \triangle B = B \triangle A$
3. *Associativity*
   (a) $A \cup (B \cup C) = (A \cup B) \cup C$
   (b) $A \cap (B \cap C) = (A \cap B) \cap C$
4. *Empty Set*
   (a) $A \cup \emptyset = A$

(b) $A \cap \emptyset = \emptyset$
(c) $A \triangle A = \emptyset$

5. *Distributivity*

   (a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
   (b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

6. *Absorption*

   (a) $A \cup (A \cap B) = A$
   (b) $A \cap (A \cup B) = A$

Cardinality

1. *Cardinality*: $|A|$ is defined as the number of distinct elements contained in A.
2. *Principle of Inclusion-Exclusion* (for two sets): $|A \cup B| = |A| + |B| - |A \cap B|$.

Power Set

1. *Power set*: $\mathcal{P}A \triangleq \{X | X \subseteq A\}$.
2. For a finite set A with $|A| = n$, $|\mathcal{P}A| = 2^n$.

Products For arbitrary sets A and B:

1. Ordered pair of elements of A and B is written as $\langle a, b \rangle$.
2. Cartesian product: $A \times B \triangleq \{\langle a, b \rangle | a \in A \wedge b \in B\}$.
3. For a finite sets A and B, $|A \times B| = |A| \times |B|$.
4. n-ary product: $A_1 \times A_2 \times \cdots \times A_n \triangleq \{\langle a_1, a_2, \ldots, a_n \rangle | \forall 1 \leq i \leq n \, (a_i \in A_i)\}$.

Partitions A partition of S is a family $A_1, A_2, \ldots, A_n$ of subsets S such that:

1. A_i is not empty: $\forall 1 \leq i \leq n \, (A_i \neq \emptyset)$.
2. The A_i cover S: $S = \cup_{i=1}^{n} A_i$.
3. The A_i are pairwise disjoint: $\forall 1 \leq i, j \leq n \, (i \neq j \implies A_i \cap A_j = \emptyset)$ (or the contrapositive).

Pigeonhole Principle If a set of n distinct objects is partitioned into k subsets, where $0 < k < n$, then at least one subset must contain at least two elements.

2 Relations

1. A *relation* R satisfies $R \subseteq A \times B$. It has *type* $A \times B$.
2. A *binary relation* on A has type A^2.

Relations can be represented as:

1. A subset of a product set.
2. A diagram with arrows between elements in two sets.
3. A directed graph, for a binary relation.
4. A matrix: for $R \subseteq A \times B$, rows are based on A and columns on B.
5. Special representations, e.g. area on the plane for binary relations on $\mathbb{R}$.

Basic Operators For $R, S \subseteq A \times B$:

1. *Union*: $R \cup S \triangleq \{\langle a, b \rangle \in A \times B | \, \langle a, b \rangle \in R \vee \langle a, b \rangle \in S\}$.
2. *Intersection*: $R \cap S \triangleq \{\langle a, b \rangle \in A \times B | \, \langle a, b \rangle \in R \wedge \langle a, b \rangle \in S\}$.
3. *Complement*: $\overline{R} \triangleq \{\langle a, b \rangle \in A \times B | \, \langle a, b \rangle \notin R\}$.
4. *Inverse*: $R^{-1} \triangleq \{\langle b, a \rangle \in A \times B | a \, R \, b\}$.

Identity $\mathrm{id}_A = \big\{\langle x, y \rangle \in A^2 | x = y\big\}$.

Composition For $R \subseteq A \times B, S \subseteq B \times C$:
$R \circ S \triangleq \{\langle a, c \rangle \in A \times C | \exists b \in B \, (a \, R \, b \wedge b \, R \, c)\}$.

Equivalence Relations The binary relation R on A is an *equivalence relation* when R is reflexive, symmetric, and transitive.

1. R is *reflexive* $\triangleq \forall x \in A \, (x \, R \, x)$.
2. R is *symmetric* $\triangleq \forall x, y \in A \, (x \, R \, y \implies y \, R \, x)$.
3. R is *transitive* $\triangleq \forall x, z \in A \, (\exists y \in A \, (x \, R \, y \wedge y \, R \, z) \implies x \, R \, z)$.

For a binary relation R on A, this is equivalent to:

1. R is *reflexive* $\iff \mathrm{id}_A \subseteq R$.
2. R is *symmetric* $\iff R = R^{-1}$.
3. R is *transitive* $\iff R \circ R \subseteq R$.

Equivalence Classes

1. For an equivalence relation R on A, for any $a \in A$, the *equivalence class* of a with respect to R is $[a]_R \triangleq \{x \in A | a \sim_R x\}$.
2. For an equivalence relation R on A, the set $\{[a]_R | a \in A\}$ forms a partition of A.

Transitive Closure *Transitive closure*: $a\, R^+\, b = \exists n \geq 1\, (a\, R^n\, b)$, i.e. $R^+ = \cup_{i \geq 1} R^i$. Contains at 'paths' in A through R. This is the smallest transitive relation containing R.

3 Functions

1. A *function* f from a set A to a set B, $f : A \to B$ is a relation $f \subseteq A \times B$ such that every element of A is related to one element in B.
2. A is the *domain* of f.
3. B is the *co-domain* of f.
4. Consider $f(a) = b$: a is the *pre-image* of b under f and b is the *image* of a under f. Every element of the domain has a single image but elements of the co-domain can have any number of pre-images.
5. An n-ary function is written $f(a_1, a_2, \ldots, a_n)$.
6. B^A denotes the set of all functions from A to B.
7. If $|A| = m$ and $|B| = n$, then $\left|B^A\right| = n^m$ or $(n+1)^m$ including partial functions.

Formal Definition of a Function † f is a function if it satisfies:

1. $f(a) = b_1 \wedge f(a) = b_2 \implies b_1 = b_2$.
2. $\forall a \in A \exists b \in B\, (f(a) = b)$.

Equality $f = g \triangleq \forall x \in A\, (f(x) = g(x))$.

Image Set

1. For $X \subseteq A$, $f[X] \triangleq \{f(a) \in B | a \in X\}$.
2. The *image set* of f is defined as $f[A] \subseteq B$.

Characteristic Functions

1. For sets $A, B \subseteq A$, the *characteristic function* of $B \subseteq A$ is the function $\chi_B : A \to \{0,1\}$ is defined as $\chi_B(a) \begin{cases} 1 & (a \in B) \\ 0 & (a \in A \backslash B) \end{cases}$.
2. For a relation $R \subseteq A_1 \times A_2 \times \cdots \times A_n$, the *characteristic function* of R is the function $\chi_R : A_1 \times A_2 \times \cdots \times A_n \to \{0,1\}$ is defined as $\chi_B(a_1, a_2, \ldots, a_n) \begin{cases} 1 & (\langle a_1, a_2, \ldots, a_n \rangle \in R) \\ 0 & (\langle a_1, a_2, \ldots, a_n \rangle \notin R) \end{cases}$.

Partial Functions A *partial function* need not satisfy clause 2 of † (and so assigns each element in the domain to at most one element in the range). Functions that satisfy clause 2 are *total functions*.

Properties of Functions For a function $f : A \to B$:

1. f is *surjective* (onto) $\triangleq \forall b \in B \exists a \in A\, (f(a) = b)$ (every element of B is in the image of f).
2. f is *injective* (one-to-one) $\triangleq \forall a_1, a_2 \in A\, (f(a_1) = f(a_2) \implies a_1 = a_2)$ (for each $b \in B$ there exists at most one $a \in A$ with $f(a) = b$).
3. f is *bijective* $\triangleq f$ is both one-to-one and onto.

Considering the cardinality of the sets A and B:

1. If f is onto, then $|A| \geq |B|$.
2. If f is one-to-one, then $|A| \leq |B|$.
3. If f is a bijection, then $|A| = |B|$.

The Pigeonhole Principle Applied to Functions For $f : A \to B$ and $X \subseteq A$, $|f[X]| \leq |X|$.

Cantor-Bernstein Theorem ‡ If there exists functions $f : A \to B$ and $g : B \to A$, both injective or both surjective, then there exists a bijection $h : A \to B$.

Operations on Functions For functions $f : A \to B$ and $g : B \to C$.

1. *Composition*: $g \circ f(a) = g(f(a))$, i.e. $g \circ f(a) = c \triangleq \exists b \in B(f(a) = b \land g(b) = c)$. Note that composition is associative. If f and g are bijections, then so is $g \circ f$.
2. *Identity*: The function $\mathrm{id}_A : A \to A$ is defined as $\mathrm{id}_A(a) = a$.
3. *Inverse*: The function $f' : B \to A$ is an inverse of f whenever: $\forall a \in A(f' \circ f(a) = a)$ and $\forall b \in B(f \circ f'(b) = b)$, i.e. $f' \circ f = id_A$ and $f \circ f' = id_B$. For f to have an inverse, f must be a bijection, and the inverse is unique.

Cardinality of Sets

1. $A \sim B \triangleq \exists f : A \to B$ (f is a bijection). The relation $\sim$ is an equivalence relation.
2. Hence if there exist functions $f : A \to B$ and $g : B \to A$, both injective or both surjective, then $A \sim B$ (by ‡).
3. We say A and B have the same *cardinality*, whenever $A \sim B$.

Cantor's Theorem For any set A, $A \not\sim \mathcal{P}A$. To prove, assume a bijection $f : A \to \mathcal{P}A$ exists. Consider $B = \{a \in A | a \notin f(a)\}$. Since f is a bijection, there exists some $b \in A$ such that $f(b) = B$. Then consider individually the cases $b \in B$ and $b \notin B$ to generate a contradiction.

4 Infinity

Countability A set A is *countable* if A is finite or $A \sim \mathbb{N}$. This is equivalent to:

1. B is countable and $A \subseteq B$.
2. There exists a surjection $f : \mathbb{N} \to A$.

Uncountability Cantor's diagonal argument produces an object that does not exist in any list. Hence any list is incomplete and so the set is uncountable.

5 Orderings

For a binary relation R on A:

1. R is a *pre-order*:R is reflexive and transitive.
2. R is *anti-symmetric*: $\forall x, y \in A(x\,R\,y \land y\,R\,x \implies x = y)$.
3. R is a *partial order relation*: R is reflexive, transitive and anti-symmetric. Usually denoted by $\leq_A$.
4. R is *irreflexive*: $\forall a \in A(\neg(a\,R\,a))$.
5. R is a *strict partial order relation*: R is irreflexive and transitive. Usually denoted by $<_A$.
6. R is a *total (linear) order*: R is a partial order that also satisfies $\forall a, b \in A(a\,R\,b \lor b\,R\,a)$.

Ordering of Products

1. Product order: $\langle a_1, b_1\rangle \leq_P \langle a_2, b_2\rangle \triangleq a_1 \leq_A a_2 \land b_1 \leq_B b_2$
2. Lexicographic order: First compare a_is, then b_is.

Hasse Diagrams Definitions:

1. If R is a partial order on set A and $a\,R\,b$ for $a \neq b$, a is a *predecessor* of b and b is a *successor* of a.
2. If a is a predecessor of b and there exists no $c \neq a, b$ with $a\,R\,c$ and $c\,R\,b$ then a is the *immediate predecessor* of b.

Hasse diagrams:

1. Record only immediate predecessors.
2. Direction of lines omitted, lines are directed 'up the page'.

Properties of Partial Orders For the partial order $\leq_A$ and $a \in A$:

1. a is minimal $\triangleq \forall b \in A(b \leq a \implies b = a)$.
2. a is least $\triangleq \forall b \in A(a \leq b)$.
3. a is maximal $\triangleq \forall b \in A(a \leq b \implies a = b)$.

4. a is greatest $\triangleq \forall b \in A\,(b \leq a)$.

Note that:

1. Any least / greatest element is a minimal / maximal element respectively.

2. Any least / greatest element is unique.

3. If A is finite and non-empty, then $\leq_A$ must have a minimal, maximal element.

4. If $\leq_A$ is a total order, where A is finite and non-empty, then it has a least, greatest element.

Well-Founded Partial Orders

1. A partial order is *well-founded* if it has no infinite decreasing chain of elements, i.e. for every infinite sequence $a_1, a_2, a_3, \ldots$ of elements in A with $a_1 \geq a_2 \geq a_3 \geq \ldots$, there exists $m \in \mathbb{N}$ such that $m \geq 1$ and $a_n = a_m$ for every $n \geq m$.

2. If two partial orders $\leq_A$ and $\leq_B$ are well-founded, then the lexicographical order $\leq_L$on $A \times B$ is also well-founded.