Discrete Mathematics

Jonathan Barrett

jonathan.barrett@cs.ox.ac.uk

Material by Andrew Ker

University of Oxford

Department of Computer Science

Computer Science, 1st year

16 lectures, Michaelmas Term 2018

What is Discrete Maths?

“The study of mathematical structures which are discrete”

What is Discrete Maths?

“The study of mathematical structures which are discrete”

Discrete objects are “not continuous”. They include

- finite sets,
- sets of whole numbers,
- finite networks,
- strings with finite alphabets,
- …

What is Discrete Maths?

“The study of mathematical structures which are discrete”

Discrete objects are “not continuous”. They include

- finite sets,
- sets of whole numbers,
- finite networks,
- strings with finite alphabets,
- …

The things we study about discrete objects include

- counting them,
- proving logical statements about them,
- designing and evaluating algorithms over them,
- measuring their fundamental complexity.

Course Aims

- Learn terminology of discrete maths, for computer science applications.

Course Aims

- Learn terminology of discrete maths, for computer science applications.

1-1, antisymmetric, associative, bag, base case, bijection, binary operator, binomial coefficients, cancellation, cardinality, cartesian product, ceiling, characteristic polynomial, closed interval, codomain, commutative, com-plement, component, composition, contrapositive, converse, counterexample, derangement, digraph, disjoint, distributivity, domain, edge, element, empty set, equivalence class, equivalence relation, exclusive, factorial, floor, function, greatest common divisor, idempotent, identity, image, independent, induction, inductive hypothesis, infix, injective, integers, intersection, interval, inverse, involution, irrational, irreflexive, member, minimal counterexample, modulus, monoid, multinomial coefficients, natural numbers, node, onto, open interval, ordered pair, parity, partial function, partition, permutation, power set, prefix, proof by contradiction, proper subset, range, rational, recurrence relation, recursive, reflexive, relation, relative complement, restriction, sequence, serial, set, subset, superset, surjective, symmetric difference, total, transitive, transitive closure, tuple, union, universe, zero, …

Course Aims

- Learn terminology of discrete maths, for computer science applications.

- Practice techniques for computing with discrete structures.

  “How many positive integers less than a million contain a digit 9?”

  “How much memory does it take to store (something)?”

  “How many steps does it take to compute (something) using (some algorithm)?”

Course Aims

- Learn terminology of discrete maths, for computer science applications.

- Practice techniques for computing with discrete structures.

  "How many positive integers less than a million contain a digit 9?"

  "How much memory does it take to store (something)?"

  "How many steps does it take to compute (something) using (some algorithm)?"

- Learn ways to **prove** mathematical statements.

  "Every third Fibonacci number is even."

  "In any set of n positive numbers all less than 2n-1, one divides another."

  "For any positive integer n, $n! \leq e^{1-n} n^n \sqrt{n}$*"*

Course Outline

- *2 lectures per week, each week a new topic.*
- *4 problem sheets + 1 vacation work.*

	topic	*associated proof method*
week 1	***Sets***	double inclusion proofs, proof by cases
week 2	***Functions***	proof of the contrapositive, proof by contradiction
week 3	***Counting***	proof techniques for counting
week 4	***Relations***	
week 5	***Sequences***	proof by induction, the minimal counterexample
week 6	***Modular Arithmetic***	pigeonhole principle
week 7	***Asymptotic Notation***	proofs of $\exists x . \forall y . S(x, y)$
week 8	***Orders***	proofs of $\forall x . \exists y . S(x, y)$

Course Outline

- *2 lectures per week, each week a new topic.*
- *4 problem sheets + 1 vacation work.*

	topic	*associated proof method*
tutorial sheet 1	***Sets***	double inclusion proofs, proof by cases
tutorial sheet 2	***Functions***	proof of the contrapositive, proof by contradiction
	Counting	proof techniques for counting
tutorial sheet 3	***Relations***	
	Sequences	proof by induction, the minimal counterexample
tutorial sheet 4	***Modular Arithmetic***	pigeonhole principle
	Asymptotic Notation	proofs of $\exists x.\forall y.S(x,y)$
vacation work	***Orders***	proofs of $\forall x.\exists y.S(x,y)$

Reading Material

Discrete Mathematics Lecture Notes.

Should contain everything you need. Distributed in lectures.
Contain "practice questions".

Kenneth A. Ross & Charles R. B. Wright. Discrete Mathematics (5th Ed)

Enormous number of exercises, comprehensive, expensive.

Ralph P. Grimaldi. Discrete and Combinatorial Mathematics (5th Ed)

Some parts too advanced, many exercises.

Amanda Chetwynd & Peter Diggle. Discrete Mathematics

Very easy to understand, cheap, only covers the first half of the course.

Peter Grossman. Discrete Mathematics for Computing Science

Slightly shallow, good CS applications, covers about 75% of the course, cheap.

Course Website

http://www.cs.ox.ac.uk/teaching/courses/2018-2019/discretemaths/

Contains:

- Lecture notes & overheads, published with about a week's delay.
- Tutorial sheets.

Discrete Mathematics

Jonathan Barrett

jonathan.barrett@cs.ox.ac.uk

Material by Andrew Ker

University of Oxford

Department of Computer Science

Chapter 1: Sets

Sets

A **set** is an **unordered** collection of **distinct** objects.

The objects in a set are called its **elements** or **members**.

If A is a set then we write $x \in A$ if x is a member of A

$x \notin A$ if x is not a member of A

Sets

A **set** is an **unordered** collection of **distinct** objects.

The objects in a set are called its **elements** or **members**.

If A is a set then we write $x \in A$ if x is a member of A

$x \notin A$ if x is not a member of A

We can define a set either by listing its members (surrounded by **braces**):

$$\{x_1, x_2, x_3\}$$

or by giving unambiguous conditions describing which objects are and are not members:

$$\{x \mid \text{some condition on } x\}$$

Some common shorthands are

$$\{x \in A \mid \text{some condition on } x\}$$

$$\{f(x) \mid \text{some condition on } x\}$$

Standard Sets

(i) $\emptyset = \{\}$, the **empty set**.

(ii) $\mathbb{N} = \{0, 1, 2, \ldots\}$, the **natural numbers** (or **nonnegative integers**).

(iii) $\mathbb{N}_+ = \mathbb{Z}_+ = \{1, 2, 3, \ldots\}$, the **positive integers**.

(iv) $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, the **integers**.

(v) $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, the **integers modulo** n (for $n = 2, 3, 4, \ldots$).

(vi) $\mathbb{Q}, = \left\{ \frac{n}{d} \;\middle|\; n \in \mathbb{Z} \text{ and } d \in \mathbb{N}_+ \right\}$, the **rational numbers**.

(vii) $\mathbb{R}$, the **real numbers**.

Warning: some books use $\mathbb{P}$ to mean the positive integers, but some use it to mean the prime numbers.

Subset and Equality

A is a **subset** of B if every member of A is also a member of B. "$A \subseteq B$"

(also pronounced "A is **contained in** B")

In the same circumstances we also say that B is a **superset** of A. "$B \supseteq A$"

Subset and Equality

A is a **subset** of B if every member of A is also a member of B. “$A \subseteq B$”

(also pronounced “A is **contained in** B”)

In the same circumstances we also say that B is a **superset** of A. “$B \supseteq A$”

A is a **proper subset** of B, or B is a **proper superset** of A, if:

- every member of A is also a member of B, and “$A \subset B$”
- some members of B are not members of A. “$B \supset A$”

(other terminology: “A is **strictly contained in** B”)

Warning: some books use the symbols $\subset$and $\varsubsetneq$ where we use $\subseteq$ and $\subset$!

Subset and Equality

A is a **subset** of B if every member of A is also a member of B. “$A \subseteq B$”

(also pronounced “A is **contained in** B”)

In the same circumstances we also say that B is a **superset** of A. “$B \supseteq A$”

A is a **proper subset** of B, or B is a **proper superset** of A, if:

- every member of A is also a member of B, and “$A \subset B$”
- some members of B are not members of A. “$B \supset A$”

(other terminology: “A is **strictly contained in** B”)

Warning: some books use the symbols $\subset$and $\subsetneq$ where we use $\subseteq$ and $\subset$!

Two sets are **equal** if they have exactly the same members.

This is equivalent to “$A = B$”

$$A \subseteq B \text{ and } B \subseteq A.$$

Operations on Sets

We can combine sets using a number of operations:

Union: $A \cup B = \{x \mid x \in A \text{ or } x \in B\}.$

Intersection: $A \cap B = \{x \mid x \in A \text{ and } x \in B\}.$

Operations on Sets

We can combine sets using a number of operations:

Union: $A \cup B = \{x \mid x \in A \text{ or } x \in B\}.$

Intersection: $A \cap B = \{x \mid x \in A \text{ and } x \in B\}.$

An Equation

For any sets A, B, and C, we believe that

$$(A \cap B) \cap C = A \cap (B \cap C)$$

How do we prove this?

Proofs

A mathematical **proof** looks like this:

Claim If ... (some hypotheses) ...
then ... (a conclusion) ...

Proof Assume ... (the hypotheses) ...
therefore ...
therefore ...
therefore ...
therefore ... (the conclusion) ... □

Every line of the proof should follow logically from the previous lines.

Proofs About Sets

To prove $A \subseteq B$ we need to show that every element of A is also an element of B.

Claim If A and B are sets
then $A \cap B \subseteq A$.

Proofs About Sets

To prove $A \subseteq B$ we need to show that every element of A is also an element of B.

Claim If A and B are sets then $A \cap B \subseteq A$.

To prove $A = B$ we need to show $A \subseteq B$ and $B \subseteq A$ (usually separately). This is called a **double inclusion proof**.

Claim If A, B, and C are sets then $(A \cap B) \cap C = A \cap (B \cap C)$.

Algebraic Laws

Union: $A \cup B = \{x \mid x \in A \text{ or } x \in B\}.$

Intersection: $A \cap B = \{x \mid x \in A \text{ and } x \in B\}.$

The following equations are true for any sets A, B, and C:

Idempotence laws:

$A \cup A = A$ $\qquad$ $A \cap A = A$

Commutativity laws:

$A \cup B = B \cup A$ $\qquad$ $A \cap B = B \cap A$

Associativity laws:

$(A \cup B) \cup C = A \cup (B \cup C)$ $\qquad$ $(A \cap B) \cap C = A \cap (B \cap C)$

Distributivity laws:

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $\qquad$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Zero and one laws:

$A \cap \emptyset = \emptyset$ $\qquad$ $A \cup \emptyset = A$

Equational Proofs

Once we know the algebraic laws, we can use them in solving problems and constructing proofs. Sometimes a proof can be constructed entirely out of algebraic laws.

Claim If A, B, C, and D are sets then $(A \cup B) \cap (C \cup D) = (A \cap C) \cup (B \cap C) \cup (A \cap D) \cup (B \cap D)$.

Proof

$$\begin{aligned}
&(A \cup B) \cap (C \cup D) \\
&\quad = ((A \cup B) \cap C) \cup ((A \cup B) \cap D) && \{\text{distributivity}\} \\
&\quad = (C \cap (A \cup B)) \cup (D \cap (A \cup B)) && \{\text{commutativity}\} \\
&\quad = ((C \cap A) \cup (C \cap B)) \cup ((D \cap A) \cup (D \cap B)) && \{\text{distributivity}\} \\
&\quad = (C \cap A) \cup (C \cap B) \cup (D \cap A) \cup (D \cap B) && \{\text{associativity}\} \\
&\quad = (A \cap C) \cup (B \cap C) \cup (A \cap D) \cup (B \cap D) && \{\text{commutativity}\}
\end{aligned}$$

Generalized Operations

Because ∪ and ∩are **associative**, we do not need parentheses in

$$A \cup B \cup C \cup D \cup \cdots$$

Useful notation is

$$\bigcup_{i=1}^{n} A_i = \{x \mid x \in A_i \text{ for some } i\} \qquad \bigcap_{i=1}^{n} A_i = \{x \mid x \in A_i \text{ for all } i\}$$

Generalized Operations

Because ∪ and ∩are **associative**, we do not need parentheses in

$$A \cup B \cup C \cup D \cup \cdots$$

Useful notation is

$$\bigcup_{i=1}^{n} A_i = \{x \mid x \in A_i \text{ for some } i\} \qquad \bigcap_{i=1}^{n} A_i = \{x \mid x \in A_i \text{ for all } i\}$$

Because ∪ and ∩are **commutative** and **idempotent**, neither the order nor repetition of the sets in

$$A \cup B \cup C \cup D \cup \cdots$$

affect the answer. This allows us to write

$$\bigcup_{i \in I} A_i = \{x \mid x \in A_i \text{ for some } i\} \qquad \bigcap_{i \in I} A_i = \{x \mid x \in A_i \text{ for all } i\}$$

Operations on Sets 2

Union: $A \cup B = \{x \mid x \in A \text{ or } x \in B\}.$

Intersection: $A \cap B = \{x \mid x \in A \text{ and } x \in B\}.$

Relative Complement: $A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}.$

Symmetric Difference:

$$A \oplus B = \{x \mid (x \in A \text{ and } x \notin B) \\ \text{or } (x \in B \text{ and } x \notin A)\}.$$

Where there is a **universe** $\mathcal{U}$, a set which contains* all other sets we are interested in, we can also define

Complement: $\overline{A} = \mathcal{U} \setminus A.$

*is a superset of

Algebraic Laws 2

Union: $A \cup B = \{x \mid x \in A \text{ or } x \in B\}.$

Intersection: $A \cap B = \{x \mid x \in A \text{ and } x \in B\}.$

Relative Complement: $A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}.$

The following equations are true for any sets A, B, and C:

Cancellation laws:

$A \setminus A = \emptyset$ $\qquad$ $A \setminus \emptyset = A$

Involution law:

$A \setminus (A \setminus B) = A \cap B$

De Morgan's laws:

$A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$ $\qquad$ $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$

Right-distributivity laws:

$(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$ $\qquad$ $(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C)$

Proving Non-Equality

To prove $A \neq B$ we need a **counterexample**: some element of A not in B, or vice versa.

Claim The left-distributive law

$$A \setminus (B \cup C) = (A \setminus B) \cup (A \setminus C)$$

is false.

Operations on Sets 3

Union: $A \cup B = \{x \mid x \in A \text{ or } x \in B\}.$

Intersection: $A \cap B = \{x \mid x \in A \text{ and } x \in B\}.$

Relative Complement: $A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}.$

Symmetric Difference: $$A \oplus B = \{x \mid (x \in A \text{ and } x \notin B) \\ \text{or } (x \in B \text{ and } x \notin A)\}.$$

Cartesian Product: $A \times B = \{(x, y) \mid x \in A \text{ and } y \in B\}.$

Power Set: $\mathcal{P}(A) = \{B \mid B \subseteq A\}.$

Note: (x, y) represents an **ordered pair**.

$(x, y) = (x', y') \quad \Leftrightarrow \quad x = x' \text{ and } y = y'.$

Operations on Sets 3

Union: $A \cup B = \{x \mid x \in A \text{ or } x \in B\}.$

Intersection: $A \cap B = \{x \mid x \in A \text{ and } x \in B\}.$

Relative Complement: $A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}.$

Symmetric Difference: $A \oplus B = \{x \mid (x \in A \text{ and } x \notin B)$ $\text{or } (x \in B \text{ and } x \notin A)\}.$

Cartesian Product: $A \times B = \{(x, y) \mid x \in A \text{ and } y \in B\}.$

Power Set: $\mathcal{P}(A) = \{B \mid B \subseteq A\}.$

Algebraic Laws 3

Distributivity laws:

$$A \times (B \cup C) = (A \times B) \cup (A \times C) \qquad A \times (B \cap C) = (A \times B) \cap (A \times C)$$

Generalized Product

Ordered pairs can be extended to n-**tuples**:

$$(x_1, x_2, \ldots, x_n)$$

Even though cartesian product is **not associative**, we still extend the × notation

$$\bigtimes_{i=1}^{n} A_i = \{(x_1, x_2, \ldots, x_n) \mid x_i \in A_i \text{ for each } i\}$$

Another useful shorthand:

$$A \times A = A^2$$

$$A \times A \times A = A^3$$

$$\vdots$$

Cardinality

The **size** of a set is called its **cardinality**. For finite sets, this is just the number of elements in the set. The cardinality of a set A is usually written

$$|A| \text{ or } \#A\,.$$

(For infinite sets, cardinality is more difficult to define.)

Interesting Diversion: Bags

A **bag** is an **unordered** collection of objects (**not** necessarily distinct).

The objects in a bag are called **elements** or **members** and the symbol $\in$is used.

Bags are usually denoted by **bag brackets**:

$$\Lbag 1, 2, 3, 3 \Rbag$$

Union, intersection, bag subtraction are defined in the obvious ways. **Some** of the algebraic laws for sets also hold for bags:

$$\begin{aligned} &A \cup B = B \cup A &\qquad& A \cap B = B \cap A \\ &(A \cup B) \cup C = A \cup (B \cup C) &\qquad& (A \cap B) \cap C = A \cap (B \cap C) \end{aligned}$$

and some do not hold:

$$\Lbag 1 \Rbag \cup \Lbag 1 \Rbag \neq \Lbag 1 \Rbag$$

$$\Lbag 1 \Rbag \cap (\Lbag 1 \Rbag \cup \Lbag 1 \Rbag) \neq (\Lbag 1 \Rbag \cap \Lbag 1 \Rbag) \cup (\Lbag 1 \Rbag \cap \Lbag 1 \Rbag)$$

Discrete Mathematics

Jonathan Barrett

jonathan.barrett@cs.ox.ac.uk

Material by Andrew Ker

University of Oxford

Department of Computer Science

End of Chapter 1