Mathematics Bootcamp Lecture Notes

Department of Statistical Sciences, University of Toronto

Emma Kroell

Last updated: July 11, 2022

Preface

These lecture notes were prepared for the Mathematics course at the inaugural Department of Statistical Sciences Graduate Student Bootcamp at the University of Toronto. The course taught an overview of necessary mathematics prerequisites to incoming statistics graduate students, with an emphasis on proofs.

These lectures are based on the following books or lecture notes:

1. *An Introduction to Mathematical Structures and Proofs* by Larry J. Gerstein
2. *A Taste of Topology* by Volker Runde
3. *Linear Algebra Done Right* by Sheldon Axler
4. *Linear Algebra Done Wrong* by Sergei Treil
5. *Introduction to Real Analysis* by William F. Trench
6. *Real Mathematical Analysis* by Charles C. Pugh
7. *Lecture notes in Mathematics for Economics and Statistics* by Piotr Zwiernik
8. *Real Analysis Lecture Notes* by Laurent Marcoux

Chapter 1 of Gerstein (2012) is used as reference for the proof technique section. Runde (2005) is the main text for the sections on set theory, metric spaces, and topology, which follow chapters 1, 2, and 3 of his book, respectively. The linear algebra content comes mostly from Axler (2015), with Treil (2017) used in some sections for an alternate perspective.

Most of the material in these notes belongs to these texts. All of these texts are available online to University of Toronto users (some to everyone).

I would like to acknowledge the assistance of Jesse Gronsbell, Stanislav Volgushev, Piotr Zwiernik, and Robert Zimmerman in developing the list of topics for the course.

Please notify me of any typos or corrections at emma.kroell@mail.utoronto.ca.

Contents

A short note on notation:

$\mathbb{N}$ denotes the whole numbers, i.e. $\mathbb{N} = \{1, 2, \ldots\}$
$\mathbb{N}_0$ denotes the non-negative integers, i.e. $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$
$\mathbb{Z}$ denotes the integers, i.e. $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$
$\mathbb{Q}$ denotes the rational numbers, i.e. $\mathbb{Q} = \{\frac{p}{q} \,|\, p, q \in \mathbb{Z} \text{ and } q \neq 0\}$
$\mathbb{R}$ denotes the real numbers
$\mathbb{C}$ denotes the complex numbers

1 Review of proof techniques

1.1 Propositional logic

Propositions are statements that could be true or false. They have a corresponding *truth value*. We will use capital letters to denote propositions. For example, "n is odd" and "n is divisible by 2" are propositions. Let's call them P and Q. Whether they are true or not (i.e. their truth value) depends on what n is.

We can negate statements: $\neg P$ is the statement "n is not odd".

We can combine statements:

- $P \wedge Q$ is the statement "n is odd and n is divisible by 2".
- $P \vee Q$ is the statement "n is odd or n is divisible by 2".

We always assume the inclusive or unless specifically stated otherwise.

Example 1.1 *Here are some statements, which we want to write in propositional logic.*

- *If it's not raining, I won't bring my umbrella.*
- *I'm a banana or Toronto is in Canada.*
- *If I pass this exam, I'll be both happy and surprised.*

For the first one, let A be the statement "it's raining" and B be the statement "I will bring my umbrella". In logic, the statement is $\neg A \implies \neg B$.

For the second, let C be the statement "I'm a banana" and let D be the statement "Toronto is in Canada". We write this as $C \vee D$.

For the third, let P be the statement "I pass this exam", let Q be the statement "I am happy", and let R be the statement "I am surprised". This one is written $P \implies (Q \wedge R)$.

1.1.1 Truth values

Example 1.2 *Write the following using propositional logic:*
If it is snowing, then it is cold out.
It is snowing.
Therefore, it is cold out.

Solution.
$P \implies Q$
P
Conclusion: Q

To examine if a statement is true or not, we use a truth table, where we write out all the possibilities.

Example 1.3 *The truth table for $P \implies Q$ where P, Q are propositions is:*

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

1.1.2 Logical equivalence

We say that two statements are *logically equivalent* if they have the same truth tables.

Example 1.4 *Let P, Q be propositions. $P \implies Q$ is logically equivalent to $\neg P \vee Q$.*

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

P	Q	$\neg P$	$\neg P \vee Q$
T	T	F	T
T	F	F	F
F	T	T	T
F	F	T	T

Theorem 1.5 (De Morgan's Laws) *Let P, Q be propositions.*

(i) $\neg(P \wedge Q)$ is logically equivalent to $\neg P \vee \neg Q$.

(ii) $\neg(P \vee Q)$ is logically equivalent to $\neg P \wedge \neg Q$.

Proving this is your first exercise.

The following fact is often useful.

Example 1.6 *$\neg(P \implies Q)$ is logically equivalent to $P \wedge \neg Q$. This follows from Example 1.4 and Theorem 1.5.*

1.1.3 Quantifiers

There are two important logical operators that we have not yet discussed. They are denoted using the following symbols: $\forall$, read as "for all" or "for each", and $\exists$, read as "there exists". We will explore their meanings, how they can help us simplify statements we need to prove, and how we prove such statements.

For all
"for all", $\forall$, is also called the universal quantifier. If $P(x)$ is some property that applies to x from some domain, then $\forall x P(x)$ means that the property P holds for every x in the domain. An example is the statement "Every real number has a non-negative square." We write this as $\forall x \in \mathbb{R}$, $x^2 \geq 0$. In logic, people often use brackets to separate parts of the logical expression, ex. $(\forall x \in \mathbb{R})(x^2 \geq 0)$.

How do we prove a for all statement? We need to take an arbitrary element of the domain, and show the property holds for that element.

There exists
"there exists", $\exists$, is also called the existential quantifier. If $P(x)$ is some property that applies to x from some domain, then $\exists x P(x)$ means that the property P holds for some x in the domain. An example is the statement that 4 has a square root in the reals. We write this as $\exists x \in \mathbb{R}$ such that $x^2 = 4$ or in proper logic notation, $(\exists x \in \mathbb{R})$ $(x^2 = 4)$.

How do we prove a there exists statement? We need to find an element in the domain for which the property holds (find an example).

There is also a special way of writing when there exists a unique element. We use $\exists!$ for this case. For example, the statement "there exists a unique positive integer such that the integer squared is 64" is written $\exists! z \in \mathbb{N}$ such that $z^2 = 64$.

Combining quantifiers
Often we will need to prove statements where we combine quantifiers.
Here are some examples:

Statement	Logical expression
Every non-zero rational number has a multiplicative inverse	$\forall q \in \mathbb{Q} \setminus \{0\}$, $\exists s \in \mathbb{Q}$ such that $qs = 1$
Each integer has a unique additive inverse	$\forall x \in \mathbb{Z}\,, \exists! y \in \mathbb{Z}$ such that $x + y = 0$
$f : \mathbb{R} \to \mathbb{R}$ is continuous at $x_0 \in \mathbb{R}$	$\forall \epsilon > 0\ \exists \delta > 0$ such that whenever $\lvert x - x_0 \rvert < \delta$, $\lvert f(x) - f(x_0) \rvert < \epsilon$

The order of quantifiers is important! Changing the order changes the meaning. Consider the following example. Which are true? Which are false?

$$\begin{gathered}\forall x \in \mathbb{R}\, \forall y \in \mathbb{R}\ x + y = 2 \\ \forall x \in \mathbb{R}\, \exists y \in \mathbb{R}\ x + y = 2 \\ \exists x \in \mathbb{R}\, \forall y \in \mathbb{R}\ x + y = 2 \\ \exists x \in \mathbb{R}\, \exists y \in \mathbb{R}\ x + y = 2\end{gathered}$$

It's also important to know how to negate logical statements that include quantifiers, as it will often help us prove or disprove the statements. The results are intuitive, but things can get complicated when we have more complex statements. The negation of a statement being true for all x is that is isn't true for at least one x. The negation of a statement being true for at least one x is that is isn't true for any x.
In summary,

$$\begin{aligned}\neg \forall x P(x) &= \exists x (\neg P(x)) \\ \neg \exists x P(x) &= \forall x (\neg P(x))\end{aligned}$$

The negations of the statements above are:

Logical expression	Negation
$\forall q \in \mathbb{Q} \setminus \{0\}$, $\exists s \in \mathbb{Q}$ such that $qs = 1$	$\exists q \in \mathbb{Q} \setminus \{0\}$ such that $\forall s \in \mathbb{Q}$, $qs \neq 1$
$\forall x \in \mathbb{Z}\,, \exists! y \in \mathbb{Z}$ such that $x + y = 0$	$\exists x \in \mathbb{Z}$ such that $(\forall y \in \mathbb{Z}, x + y \neq 0) \vee (\exists y_1, y_2 \in \mathbb{Z}$ such that $y_1 \neq y_2 \wedge x + y_1 = 0 \wedge x + y_2 = 0\ )$
$\forall \epsilon > 0\ \exists \delta > 0$ such that whenever $\lvert x - x_0 \rvert < \delta$, $\lvert f(x) - f(x_0) \rvert < \epsilon$	$\exists \epsilon > 0$ such that $\forall \delta > 0$, $\lvert x - x_0 \rvert < \delta$ and $\lvert f(x) - f(x_0) \rvert \geq \epsilon$

Note that we use De Morgan's laws (Theorem 1.5), as well as the negation of an implication (Example 1.6). What do these negations mean in English?

1.2 Types of proof

1.2.1 Direct proof

In a direct proof, our approach is to use the definition and known results.

Example 1.7 *The product of an even number with another integer is even.*

To prove this statement, we will use the definition of even. First we state that definition.

Definition 1.8 *We say that an integer n is* even *if there exists another integer j such that $n = 2j$.*
We say that an integer n is odd *if there exists another integer j such that $n = 2j + 1$.*

Now we prove the example directly.

Proof. Let $n, m \in \mathbb{Z}$, with n even. By definition, there $\exists\ j \in \mathbb{Z}$ such that $n = 2j$. Then

$$nm = (2j)m = 2(jm)$$

Therefore nm is even by definition. □

Here is another example, which uses the concept of divisibility.

Definition 1.9 *Let $a, b \in \mathbb{Z}$. We say that "a divides b", written $a|b$, if the remainder is zero when b is divided by a, i.e. $\exists j \in \mathbb{Z}$ such that $b = aj$.*

Example 1.10 *Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. Prove that if $a|b$ and $b|c$, then $a|c$.*

Proof. Let $a, b, c \in \mathbb{Z}$. Suppose $a|b$ and $b|c$. Then by definition, there exists $j, k \in \mathbb{Z}$ such that $b = aj$ and $c = kb$. Combining these two equations gives $c = k(aj) = a(kj)$. Thus $a|c$ by definition. □

1.2.2 Proof by contrapositive

Sometimes instead of proving an implication $P \implies Q$ directly, it is easier to prove $\neg Q \implies \neg P$. This is called the contrapositive. First, we show that these two statements are logically equivalent using truth tables.

$P \implies Q$

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

$\neg Q \implies \neg P$

P	Q	$\neg P$	$\neg Q$	$\neg Q \implies \neg P$
T	T	F	F	T
T	F	F	T	T
F	T	T	F	F
F	F	T	T	T

Note that $\neg P \implies \neg Q$ is *not* logically equivalent to $P \implies Q$ (can you think of an example?). This is a common mistake.

Here is an example of a statement that is easier to prove using the contrapositive as opposed to directly.

Example 1.11 *If an integer squared is even, then the integer is itself even.*

Proof. We prove the contrapositive. Let n be odd. Then there exists $k \in \mathbb{Z}$ such that $n = 2k + 1$. We compute

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Thus n^2 is odd. □

1.2.3 Proof by contradiction

Another proof technique is to assume something we know to be (or think to be) false, and then try to derive a contradiction. A contradiction is something that is impossible, like 0=1 or showing that a number is both odd and even.

In sum, to prove that a statement P is true by contradiction, we assume $\neg P$ is true, derive a contradiction, and conclude that P is true. Here is an example.

Example 1.12 *The sum of a rational number and an irrational number is irrational.*

Proof. Let $q \in \mathbb{Q}$ and $r \in \mathbb{R} \setminus \mathbb{Q}$. Suppose in order to derive a contradiction that their sum is rational, i.e. $r + q = s$ where $s \in \mathbb{Q}$. But then $r = s - q \in \mathbb{Q}$. Contradiction. Therefore the sum of a rational number and an irrational number is irrational. □

1.2.4 Summary

In sum, to prove $P \implies Q$:

Direct proof:	assume P, prove Q
Proof by contrapositive:	assume $\neg Q$, prove $\neg P$
Proof by contradiction:	assume $P \wedge \neg Q$ and derive something that is impossible

1.2.5 Induction

Finally, we consider a special proof technique for proving statements about the natural numbers (or subsets of them of certain forms). It is based on the following theorem, which we state without proof.

Theorem 1.13 (Well-ordering principle for $\mathbb{N}$) *Every nonempty set of natural numbers has a least element.*

Because of the well-ordering principle, we can prove something holds for the natural numbers by proving it holds for the smallest one, and then creating a logical ladder linking them together as follows:

Theorem 1.14 (Principle of mathematical induction) *Let n_0 be a non-negative integer. Suppose P is a statement about positive integers n such that*

1. *(base case) $P(n_0)$ is true*
2. *(induction step) For every integer $k \geq n_0$, if $P(k)$ is true, then $P(k+1)$ is true.*

Then $P(n)$ is true for every integer $n \geq n_0$

Here is an example of a proof by induction.

Example 1.15 *$n! > 2^n$ if $n \geq 4$.*

Proof. We prove this by induction on n.
Base case: Let $n = 4$. Then $n! = 4! = 24 > 16 = 2^4$.
Inductive hypothesis: Suppose for some $k \geq 4$, $k! > 2^k$.
Then

$$(k+1)! = (k+1)k! > (k+1)2^k > 2(2^k) = 2^{k+1}.$$

Thus the statement holds by induction on n. □

Sometimes we use a different version of induction, called strong induction.

Theorem 1.16 (Principle of strong mathematical induction) *Let n_0 be a non-negative integer. Suppose P is a statement about positive integers n such that*

1. *(base case) $P(n_0)$ is true*
2. *(induction step) For every integer $k \geq n_0$, if $P(m)$ is true for every integer m with $n_0 \leq m \leq k$, then $P(m+1)$ is true.*

Then $P(n)$ is true for every integer $n \geq n_0$.

Next, we will consider an example where it is much simpler to use the strong version of induction than the regular one. First, we recall the definition of a prime number.

Definition 1.17 *A positive integer p is prime if p has exactly two positive integer factors: 1 and p. Note that 1 is not prime. We can write this as*

$$p > 1 \textit{ is prime if } \forall\, a, b \in \mathbb{N},\, p = ab \implies (a = 1 \textit{ or } b = 1).$$

We want to prove the existence part of the Fundamental Theorem of Arithmetic, that every integer greater than or equal to 2 has a prime factorization. The fact that such a factorization is unique is left as an exercise.

Example 1.18 *Every integer $n \geq 2$ can be written as the product of primes.*

Proof. We prove this using the Principle of Strong Mathematical Induction on n.
Base case: $n = 2$ is prime.
Inductive hypothesis: Suppose for some $k \geq 2$ that one can write every integer n such that $2 \leq n \leq k$ as a product of primes.
We must show that we can write $k+1$ as a product of primes.
Case 1: if $k+1$ is prime, then we are done.
Case 2: if $k+1$ is not prime, then by Definition 1.17, there exists $a, b \in \mathbb{N}$ such that $k+1 = ab$ where $a, b \neq 1$. Then it must also be the case that $a, b \leq k$.
By the inductive hypothesis, we can write a and b as products of primes, i.e. $\exists p_1, \ldots p_\ell, q_1, \ldots q_m$, all prime, such that

$$a = p_1 \cdots p_\ell, \qquad b = q_1 \cdots q_m.$$

Then

$$k+1 = ab = p_1 \cdots p_\ell \, q_1 \cdots q_m,$$

therefore we can write $k+1$ as a product of primes.
Thus the claim holds by strong induction. □

The Principle of Strong Mathematical Induction and the Principle of Mathematical Induction are logically equivalent, but sometimes it is easier to use one or the other, as we saw.

1.3 Exercises

1. Prove De Morgan's Laws for propositions: $\neg(P \wedge Q) = \neg P \vee \neg Q$ and $\neg(P \vee Q) = \neg P \wedge \neg Q$ (Hint: use truth tables).

2. Write the following statements and their negations using logical quantifier notation and then prove or disprove them:

   (i) Every odd integer is divisible by three.

   (ii) For any real number, twice its square plus twice itself plus six is greater than or equal to five. *(You may assume knowledge of calculus.)*

   (iii) Every integer can be written as a unique difference of two natural numbers.

3. Prove the following statements:

   (i) If $a|b$ and $a, b \in \mathbb{N}$ (positive integers), then $a \leq b$.

   (ii) If $a|b$ and $a|c$, then $a|(xb + yc)$, where $a, b, c, x, y \in \mathbb{Z}$.

   (iii) Let $a, b, n \in \mathbb{Z}$. If n does not divide the product ab, then n does not divide a and n does not divide b.

4. Prove that for all integers $n \geq 1$, $3|(2^{2n} - 1)$.

5. Prove the Fundamental Theorem of Arithmetic, that every integer $n \geq 2$ has a unique prime factorization (i.e. prove that the prime factorization from the last proof is unique).

1.4 References

Most of this content may be found in Chapter 1 of [Ger12], though many of the examples are my own. [Lak16] is also a great resource, but sadly it is not freely available online or at U of T.

References

[Ger12] Larry J. Gerstein. *Introduction to Mathematical Structures and Proofs*. Undergraduate Texts in Mathematics. 2012. URL: https://link-springer-com.myaccess.library.utoronto.ca/book/10.1007/978-1-4614-4265-3l.

[Lak16] Tamara J. Lakins. *The Tools of Mathematical Reasoning*. Pure and Applied Undergraduate Texts. 2016.