Let’s be safe

Please sit so that there is at least one empty set between you and any student on your left or right.

MATH1005/MATH6005: Discrete Mathematical Models

Adam Piggott

Semester 1, 2021

Preface to the course

An acknowledgement of country

We acknowledge and celebrate the Ngunnawal people, the First Australians on whose traditional lands we meet. We pay our respect to the elders, past and present.

Course material

The lecture notes for the course are intended to be self-contained. Notes will be posted to our Wattle page immediately after the lecture, if not before. For most students, these notes, the workshop materials and the web will be sufficient.

If you would like an alternative presentation of the material, our optional text is [1].

- Copies of the text are on 2-hour loan in the library.
- From the publisher: “Students who wish to purchase their own eBook copies they can do so through `https://au.cengage.com/` Use the coupon code TENOFF to receive a discount at checkout.”

Credits

This course has been developed by a number of mathematicians over more than a decade. Contributing authors include:

- Judy-anne Osborne
- Pierre Portal
- Malcolm Brooks
- Adam Piggott

The mathematics in this course has been developed over millennia. Credit for discovery will be given only occasionally.

Other notes

- You must check the Wattle page, particularly the announcements, often.
- MATH1005 Assessment: workshop participation and weekly assignments starting in week 3, a mid-semester exam in week 7, a final exam.
- MATH6005 Assessment: weekly assignments starting in week 3, three graduate assignments, a mid-semester exam in week 7, a final exam.
- All students should sign up for a workshop through the course Wattle page.
- In weeks 3 and 8, the Monday lecture will not be held and Monday workshops will be rescheduled.

Why study discrete mathematical models?

What are discrete mathematical models?

Discrete mathematical models are abstract representations of processes and objects, the steps or units of which can be indexed by the non-negative integers. In particular, we avoid continua (like the open interval $(0, 1)$).

Discrete mathematics is the study of discrete mathematical models.

Q: Is completing a Sudoku puzzle an exercise in discrete mathematics?

Computing and discrete mathematical models

Discrete mathematics and computer science go hand-in-hand because ...

Q: Describe an abstract model of the memory of a computer. That is, how do you think about memory?

Q: Do you think about computers working in continuous time or discrete time ("clock cycles")?

Q: Can the interval $(0, 1)$ be modeled inside a computer?

Discrete mathematics and computer science

In 1974, Knuth wrote:

> "Discrete mathematics, especially combinatorial theory, has been given an added boost by the rise of computer science, in addition to all the other fields in which discrete mathematics is currently being extensively applied." [2]

This paper by Knuth is now available in the Week 1 section of our Wattle page. Please read the first 4 sections (pages 323-329) of the paper before lecture 2.

Discrete mathematics and computer scientists

Let's consider the educational background of some A. M. Turing Award laureates.

- Donald Knuth (1974)
- Andrew Chi-Chih Yao (2000)
- Barbara Liskov (2008)
- Shafi Goldwasser(2012)
- David Patterson (2017)

References

[1] Susanna S. Epp. *Discrete Mathematics with Applications: Metric Version*. Cengage Learning, 5th edition, 2019. ISBN: 9780357114087.

[2] Donald E. Knuth. Computer science and its relation to mathematics. *Amer. Math. Monthly*, 81:323–343, 1974.

Section A: The language of mathematics and computer science

Part 1: Logic

Statements: The basic unit of logic

A **statement** is a sentence that is true or false but not both.

Statements: The basic unit of logic

A **statement** is a sentence that is true or false but not both.

Some sentences that are statements:

- Australia is in the Southern Hemisphere.
- Tropical storms spin clockwise in the Southern Hemisphere.
- Canberra is in New Zealand.
- $3 > 2$

Some sentences that are not statements:

- How are you going? (question)
- Canberra is a better city than Sydney. (ambiguous)
- Wake up! (instruction/advice)
- This statement is false. (neither true nor false; self-referencing)

Compound statements

Logical connectives such as ‘and’, ‘or’, ‘not’, ‘if-then’,‘if and only if’ may be used to glue the statements together to make new statements.

Compound statements are statements built from other statements using logical connectives.

Example: Australia is in the Southern Hemisphere and tropical storms spin clockwise in the Southern Hemisphere.

Example: If 2 divides 4238 and 3 divides 4238, then 6 divides 4238.

Compound statements

Sometimes the way a compound statement is built from other statements is less clear, because our everyday use of language does not make the logical structure obvious. For example, the word ‘not’ sometimes causes confusion because of its placement.

Examples of compound statements

Q: In each of the following examples, identify clearly the way the statement is built from other statements using logical connectives:

- Australia is in the Southern hemisphere and tropical storms spin clockwise in the Southern Hemisphere.
- Australia is in the Southern Hemisphere and Canberra is not in New Zealand.
- I don’t like either the one or the other.

Compound statements

Takeway: What makes for nice spoken or written language, may not necessary make the logical structure of a compound statement most clear. Worse, the everyday use of language can be ambiguous.

Mathematicians and computer scientists must agree upon the meaning of logical connectives, and must be proficient at recognising the way that compound statements are built from simpler statements, so that we can communicate effectively (human-to-human, and human-to-machine).

How to introduce a symbol for a statement

When you first learned algebra, you learned that it was useful to use variables to make abstract statements about relationships between numbers. In logic, we sometime save time and space, and clarify the logical structure of a compound statement, by introducing symbols as names for statements.

For example, we write

$$p: \text{ Australia is in the Southern Hemisphere}$$

to mean that the symbol p now represents the statement "Australia is in the Southern Hemisphere."

Statement variables and statement forms

We can also use variables to represent arbitrary statements. When a variable represents an arbitrary statement, it is called a **statement variable**.

We have symbols for various logical connectives (such as $\neg$ for ‘not’, $\wedge$ for ‘and’, $\vee$ for ‘or’). We will define these properly in a moment.

An expression built using statement variables, parentheses and logical connectives is called a **statement form** if the expression becomes a statement when actual statements are substituted for the component statement variables.

Examples of statement forms

Example: Let p and q be statement variables.

The expression $q \vee \neg(p \wedge q)$ is a statement form.

The expression $p \neg \wedge q$ is not a statement form (just like $x + \times\ y$ is not an algebraic expression).

About statement forms

The value of the algebraic expression $x \times y + y$ depends on the values taken by x and y. You need to understand the multiplication and addition operations, and the order of precedence among operations, to figure out the value of the expression.

Analogously, the **truth value** of the statement form $q \vee \neg(p \wedge q)$ depends on the truth values taken by p and q. You need to understand the logical connectives $\neg$, $\wedge$, $\vee$ and the order of precedence among them to figure out the truth value of the statement form.

Truth tables

We are now ready to define logical connectives. We shall do so using truth tables. A **truth table** records the truth value taken by a statement form for each possible combination of truth values taken by the statement variable appearing in the statement form.

A logical connective: NOT

If p is a statement variable, the **negation** of p is read “not p”, denoted $\neg p$, and defined by the following truth table:

p	$\neg p$
T	F
F	T

A logical connective: AND

If p and q are statement variables, the **conjunction** of p and q is read "p and q", denoted $p \wedge q$, and defined by the following truth table:

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

A logical connective: OR

If p and q are statement variables, the **disjunction** of p and q is read "p or q", denoted $p \vee q$, and defined by the following truth table:

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

A logical connective: XOR

If p and q are statement variables, the **exclusive disjunction** of p and q is read "p or q but not both", denoted $p \oplus q$, and defined by the following truth table:

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

Note: Grammatically, the words 'and' & 'but' are both conjunctions, so are both interpreted as AND in logic. You could read $p \oplus q$ as "p or q and not both."

A logical connective: IMPLIES

If p and q are statement variables, the **conditional** of q by p is read "if p then q" or "p implies q", denoted $p \to q$, and defined by the following truth table:

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

There is extra vocabulary associated with conditional. In the statement form $p \to q$, we call p the **hypothesis** (or antecedent) and q the **conclusion** (or consequent).

Understanding IMPLIES

Pay careful attention to the truth table for a conditional. On first sight, some find the last two lines surprising. Spend some time making sure you know the details of the definition.

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

It sometimes helps to use language to emphasize *why* a conditional is true. When the hypothesis in a conditional is false, we say that the conditional is **vacuously true**.

A logical connective: IFF

If p and q are statement variables, the **biconditional** of p and q is read "p if and only if q", denoted $p \leftrightarrow q$, and defined by the following truth table:

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Order of precedence among logical connectives

When evaluating a statement form:

- Obey parentheses over any precedence rule
- Evaluate $\neg$ first
- Evaluate $\wedge$, $\vee$ and $\oplus$ second. When two or more are present, parentheses may be needed
- Evaluate $\rightarrow$ and $\leftrightarrow$ third. When both are present, parentheses may be needed.

When writing statement forms, you must use parentheses to avoid ambiguity. For example, you should write $p \wedge (q \vee r)$ rather than $p \wedge q \vee r$.

Example: Truth table for a complex statement form

Q: Write a truth table for $(p \wedge q) \vee (\neg p \wedge \neg r)$.

First we note that:

- Our table needs a row for each combination of truth values among the statement variables. Since there are three statement variables in the statement form, our table will need $2^3 = 8$ rows.
- We need to obey the order of precedence among logical connectives as we evaluate the truth value of the statement form.

We shall present two ways to lay out our work.

Method 1: Use construction columns

p	q	r	$p \wedge q$	$\neg p$	$\neg r$	$\neg p \wedge \neg r$	$(p \wedge q) \vee (\neg p \wedge \neg r)$
T	T	T	T	F	F	F	T
T	T	F	T	F	T	F	T
T	F	T	F	F	F	F	F
T	F	F	F	F	T	F	F
F	T	T	F	T	F	F	F
F	T	F	F	T	T	T	T
F	F	T	F	T	F	F	F
F	F	F	F	T	T	T	T

An advantage of this method is that you leave a record of your working. A disadvantage is that is can take a lot of room on the page.

Method 2: Align truth values under connectives

p	q	r	$(p \wedge q) \vee (\neg p \wedge \neg r)$				
T	T	T	T	$\mathbf{T}$	F	F	F
T	T	F	T	$\mathbf{T}$	F	F	T
T	F	T	F	$\mathbf{F}$	F	F	F
T	F	F	F	$\mathbf{F}$	F	F	T
F	T	T	F	$\mathbf{F}$	T	F	F
F	T	F	F	$\mathbf{T}$	T	T	T
F	F	T	F	$\mathbf{F}$	T	F	F
F	F	F	F	$\mathbf{T}$	T	T	T

If you use this method:

- Be careful because your work leaves less of a record of how you did it.
- Bold, circle or highlight the column with the final result.

Tautologies

A statement form that is true regardless of the truth values of its variables is called a **tautology**. A statement whose form is a tautology is also called a **tautology**.

We can show that a statement form is a tautology by making a truth table. We can show that a statement is a tautology by making a truth table for the corresponding statement form.

Showing that a statement (form) is a tautology

Example: The statement form $p \vee \neg p$ is a tautology, as shown by:

p	$\neg p$	$p \vee \neg p$
T	F	T
F	T	T

Example: The statement "$\sqrt{2}$ is negative or non-negative" is a tautology because:

- it is an instance of the statement form $p \vee \neg p$ with

$$p : \sqrt{2} \text{ is negative,}$$

- the statement form $p \vee \neg p$ is a tautology.

Contradiction

A statement form that is false regardless of the truth values of its variables is called a **contradiction**. A statement whose form is a contradiction is also called a **contradiction**.

We can show that a statement form is a contradiction by making a truth table. We can show that a statement is a contradiction by making a truth table for the corresponding statement form.

Logical equivalence

When two statement forms f, g have identical truth tables we say they are **logically equivalent** and write $f \equiv g$.

(ALTERNATIVE DEFINITION: When f, g are statement forms and $f \leftrightarrow g$ is a tautology, we say that f and g are **logically equivalent** and write $f \equiv g$.)

Knowing some logical equivalences allows us to replace complicated statement forms by simpler, logically equivalent, statement forms.

Some well-known logical equivalences are shown on the next slide.

From page 49 of the optional text

Theorem 2.1.1 Logical Equivalences

Given any statement variables p, q, and r, a tautology $\mathbf{t}$ and a contradiction $\mathbf{c}$, the following logical equivalences hold.

1. *Commutative laws:*	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
2. *Associative laws:*	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
3. *Distributive laws:*	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
4. *Identity laws:*	$p \wedge \mathbf{t} \equiv p$	$p \vee \mathbf{c} \equiv p$
5. *Negation laws:*	$p \vee \sim p \equiv \mathbf{t}$	$p \wedge \sim p \equiv \mathbf{c}$
6. *Double negative law:*	$\sim(\sim p) \equiv p$	
7. *Idempotent laws:*	$p \wedge p \equiv p$	$p \vee p \equiv p$
8. *Universal bound laws:*	$p \vee \mathbf{t} \equiv \mathbf{t}$	$p \wedge \mathbf{c} \equiv \mathbf{c}$
9. *De Morgan's laws:*	$\sim(p \wedge q) \equiv \sim p \vee \sim q$	$\sim(p \vee q) \equiv \sim p \wedge \sim q$
10. *Absorption laws:*	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
11. *Negations of* $\mathbf{t}$ *and* $\mathbf{c}$:	$\sim\mathbf{t} \equiv \mathbf{c}$	$\sim\mathbf{c} \equiv \mathbf{t}$

Note: The text uses $\sim$ for negation instead of $\neg$.

Example: An equivalent form for XOR

Q: Justify the earlier claim that $p \oplus q \equiv (p \vee q) \wedge \neg(p \wedge q)$.

Example: An equivalent form for XOR

Q: Justify the earlier claim that $p \oplus q \equiv (p \vee q) \wedge \neg(p \wedge q)$.

We compute a truth table:

p	q	$p \oplus q$	$p \vee q$	$p \wedge q$	$\neg(p \wedge q)$	$(p \vee q) \wedge \neg(p \wedge q)$
T	T	F	T	T	F	F
T	F	T	T	F	T	T
F	T	T	T	F	T	T
F	F	F	F	F	T	F

Because the entries in column 3 and column 7 agree in every row, the truth table above establishes that $p \oplus q \equiv (p \vee q) \wedge \neg(p \wedge q)$.

Example: Another equivalent form for XOR

Q: Show that $p \oplus q \equiv (p \wedge \neg q) \vee (\neg p \wedge q)$

Example: Another equivalent form for XOR

Q: Show that $p \oplus q \equiv (p \wedge \neg q) \vee (\neg p \wedge q)$

We compute a truth table:

p	q	$p \oplus q$	$\neg p$	$\neg q$	$p \wedge \neg q$	$\neg p \wedge q$	$(p \wedge \neg q) \vee (\neg p \wedge q)$
T	T	F	F	F	F	F	F
T	F	T	F	T	T	F	T
F	T	T	T	F	F	T	T
F	F	F	T	T	F	F	F

Because the entries in column 3 and column 8 agree in every row, the truth table above establishes that $p \oplus q \equiv (p \wedge \neg q) \vee (\neg p \wedge q)$.

Your homework between now and lecture 2

- Master the vocabulary introduced in this lecture and practice making truth tables for complex statement forms
- Read the first 4 sections (pp. 323-329) of Knuth's paper referenced on slide #5 (the paper is available in Wattle), and prepare bullet points in response to the following "Identify three interesting observations/points made by Knuth in the first 4 sections of the paper."
- Use Sudoku.com. Announce your best time (and the level of difficulty) on the course Wattle forum.