# Foundations of computation

DRAFT EDITION

# Foundations of computation

DRAFT EDITION

David W. Rosoff
The College of Idaho

September 1, 2023

**Website**: example.org



[1] creativecommons.org/licenses/by-sa/4.0

# Contents

# Chapter 1

# Chapter title

## 1.1 Proofs

### Objectives

- 

### 1.1.1 Class Activities

**Activity 1.1.1** Negate the following statement:

Mike and Karen are tall.

Choose the correct statement:

⊙ Mike is not tall, or Karen is not tall

⊙ Mike is tall, or Karen is tall

⊙ Mike is not tall, and Karen is not tall

⊙ Mike is tall, and Karen is tall

**Solution**. Mike and Karen are tall. Let $p$ be the statement Mike is tall Let $q$ be the statement Karen is tall First, translate the statement into formal logic. In this statement, $p$ is true, and $q$ is true. Therefore, the correct answer is $p\boldsymbol{and}q$, or $p \wedge q$. Now, negate the statement. $\sim(p \wedge q) \equiv (\sim p \vee \sim q)$ Thus, the answer is $\sim p \vee \sim q$ Recall what $p$ and $q$ represent: p: Mike is tallq: Karen is tall From $\sim p \vee \sim q$, we get Mike is not tall, or Karen is not tall.

**Activity 1.1.2** Buttercup knows whether or not Westley is lying. She promises that if Westley is lying, she will give you a cookie. Buttercup always keeps her promises.

Suppose she does not give you a cookie; what can you conclude?

(☐ Westley is lying. ☐ Westley is not lying. ☐ Not enough information to determine.)

Suppose she gives you a cookie; what can you conclude?

(☐ Westley is lying. ☐ Westley is not lying. ☐ Not enough information to determine.)

**Answer 1**. Westley is not lying.

**Answer 2**. Not enough information to determine.

**Solution**.

**Activity 1.1.3** Negate the following statement:

If Mary fails her classes, then she cannot graduate.
p: Mary fails her classes
q: Mary can graduate
Write the statement in formal logic:

- $\sim p \to q$
- $q \to p$
- $p \to \sim q$
- $p \to q$

Negate the logic:

- $\sim p \wedge \sim q$
- $\sim p \wedge q$
- $p \wedge q$
- $\sim p \vee \sim q$

Rewrite the negated logic in English

- Mary does not fail her classes or she cannot graduate
- Mary does not fail her classes and she cannot graduate
- Mary does not fail her classes and she can graduate
- Mary fails her classes and she can graduate

**Solution**. If Mary fails her classes, then she cannot graduate.p: Mary fails her classesq: Mary can graduate
In this statement, if $p$ is true, then $q$ is false. This is an *implies* relationship. Thus, the answer is $p \to \sim q$ Now, negate the statement. In order to negate this statement, first translate it into an *or* statement to get rid of the *implies* operator. $p \to \sim q \equiv \sim p \vee \sim q \sim(\sim p \vee \sim q) \equiv p \wedge q$ Thus, the answer is $p \wedge q$ Recall what $p$ and $q$ represent: p: Mary fails her classesq: Mary can graduate From $p \wedge q$, we get Mary fails her classes, and she can graduate.

**Activity 1.1.4** Negate the following statement.

Billy and Bob are applying for the same job, but only one can succeed.
p: Billy gets the job
q: Bob gets the job
Choose the correct statement:

- $\sim(p \wedge q)$
- $\sim(p \vee q)$
- $p \vee q$
- $p \wedge q$

**Solution**. Billy and Bob are applying for the same job, but only one can succeed.p: Billy gets the jobq: Bo
First, translate the statement into formal logic. In this statement, $p$ can be true, xor $q$ can be true, or neither can be true. The key here is that while either one ***can*** succeed, there is no guarantee of success. The expression is then equal to $\sim(p \wedge q)$ Now, negate the statement. $\sim(\sim(p \wedge q)) \equiv \sim\sim(p \wedge q) \equiv p \wedge q$ The

answer is then $p \wedge q$ As an extra exercise, what would this statement translate to in English?

**Activity 1.1.5** Which of the following are equivalent to $\sim(A \vee \sim B)$? Select all that apply.

A. $\sim A \vee B$

B. $\sim A \wedge B$

C. $A \vee \sim B$

D. $A \wedge \sim B$

**Activity 1.1.6** Which of the following are equivalent to the contrapositive of the logical expression $A \vee \sim B \to C \vee \sim D$? Select all that apply.

A. $C \vee \sim D \to A \wedge \sim B$

B. $\sim(C \vee \sim D) \to \sim(A \wedge \sim B)$

C. $\sim(A \vee \sim B) \to \sim(C \vee \sim D)$

D. $\sim A \vee B \to \sim C \wedge D$

**Activity 1.1.7** We say a set $A$ is **finite** if there is a nonnegative integer $n$ such that the proposition

$$A \text{ has } n \text{ elements} \tag{1.1.1}$$

is true. If $A$ is a finite set, then $|A|$ denotes the size of $A$, the number of its elements.

A one-to-one correspondence or bijection is a function that can be reversed. Given a function $f\colon A \to B$, you can tell that $f$ is a bijection if it pairs each "input" (argument) to a *unique* output (value).

**(a)** Let $A$ be a finite set. How many functions are there with domain $A$ and codomain $\overline{\mathbf{2}} = \{0, 1\}$?Try listing all possibilities for $|A| = 1, 2, 3$. A pattern should emerge. Once you think you see it, try to explain why that is the answer. The lists you made for the small examples should help you see the "general" case.

**(b)** Establish a one-to-one correspondence (i.e., a bijection) between the set of functions $A \to \overline{\mathbf{2}}$ and the power set $2^A = \{B : B \subseteq A\}$.The "inputs" of your bijection could be the functions $A \to \overline{\mathbf{2}}$ and the "outputs" the elements of the set $2^A$.Define a function

$$\mathrm{ev}_1\colon \{f : f \text{ is a function } A \to \overline{\mathbf{2}}\} \to 2^A$$

by the equation $\mathrm{ev}_1(f) = \{x \in A : f(x) = 1\}$. We will show that $\mathrm{ev}_1$ is a bijection. Bijections are functions with two properties:

(a) If $s \neq t$ then $G(s) \neq G(t)$ (no overlap/collision; at most one inbound arrow for each codomain element)

(b) For each $y$ in the codomain, there is $x$ in the domain such that $G(x) = y$ (every codomain element "covered"; at least one inbound arrow for each codomain element)

Suppose that $f$ and $g$ are distinct functions $A \to \overline{\mathbf{2}}$. We need to show that $\mathrm{ev}_1(f) \neq \mathrm{ev}_1(g)$. The first is the subset of $A$ on which $f$ takes the value 1. The second is the same set, but for $g$. Since $f \neq g$, there is some $x \in A$ where $f(x) \neq g(x)$. Since the only possible values of these functions are 0 and 1, it follows that exactly one of $f(x)$ and $g(x)$ is equal to 1. Hence $x$ is a member of $\mathrm{ev}_1(f)$ or $\mathrm{ev}_1(g)$, but not both. This shows that $\mathrm{ev}_1$ has the first property of a bijection.

To obtain the second, let us choose an arbitrary element $S \in 2^A$. This $S$ is just a subset of $A$. We must show that there exists a function $h$ such that $\mathrm{ev}_1(h) = S$. We may of course define

$$h(x) = \begin{cases} 0 & \text{if } x \notin S \\ 1 & \text{if } x \in S \end{cases}$$

and then we see at once that $h$ has the desired property. We have now shown that $\mathrm{ev}_1$ has both properties of a bijection.

**(c)** Conclude that $|\{f\colon A \to \overline{\mathbf{2}}\}| = |2^A|$, and identify the common value of these expressions. (Your answer will depend on $A$.)Since we have seen a bijection between these sets, they have the same size. We listed all the binary functions on $n$ variables; there are $2^n$ of them, so there must be $2^n$ subsets of $A$ as well. Observe these combine to say

$$|2^A| = 2^{|A|}$$

for every finite set $A$.

## 1.2 Induction

### Objectives

**Theorem 1.2.1** *Let $A$ be a nonempty subset of the natural numbers $\mathbb{N}$ satisfying*

1. $0 \in A$*; and*
2. *If $n \in \mathbb{N}$ and $n \in A$, then $n + 1 \in A$.*

*Then $A = \mathbb{N}$.*

We usually apply the induction theorem in a highly implicit way. It is only invoked by name in introductory texts like this one. We have a sequence of theorems we wish to prove by induction. Usually we are too lazy to speak this way and we say we are proving one theorem, but about every natural number instead of a specific one (or about trees of arbitrary height instead of trees of height $n$). Each theorem in our sequence has a hypothesis $P_n$ and a conclusion $Q_n$. Often all of the $P_n$ are the same, but it doesn't hurt anything to let them be different. It happens even more often that all of the $Q_n$ are specializations of a statement about integers to a specific integer. What we do when we write a proof by induction is to apply the induction theorem to the set $S$ defined by

$$S = \{n \in \mathbb{N} : P_n \implies Q_n\},$$

that is, the set of natural numbers (or e.g. tree heights) for which our theorem holds. If we can show the hypotheses of the induction theorem apply to the set $S$, our proof is complete, because the conclusion of the induction theorem then entails that $S = \mathbb{N}$.

This is what I meant in class when I spoke of an "argument machine". As stated above, none of this framework is ever explicitly mentioned in practice. In undergraduate books, it is considered enough to mention induction, prove a "base case" and an "induction step" or "inductive case" (two phrases for the same thing), and voilà! The proof is complete.

Thus, the "induction framework" consists of arranging your argument so that the sequences $P_n$ and $Q_n$ are clear. We call the theorem "$P_0 \implies Q_0$" the "base case". This theorem could also be stated as "$0 \in S$".

The inductive case is always phrased as a conditional. "*If* $n$ is a natural number that is in $S$, *then* $n+1$ is also in $S$." If you recall the definition of $S$, you will see that this conditional is equivalent to

$$(P_n \implies Q_n) \implies (P_{n+1} \implies Q_{n+1}).$$

So, we usually formulate our induction step in the latter way. My *induction hypothesis* would be "$P_n$ implies $Q_n$". From this hypothesis I would attempt to deduce the conclusion, "$P_{n+1}$ implies $Q_{n+1}$".

As a final thought, I should tell you that in our real writing, we *don't* usually assign values like $P_n$ to specific predicates like "6 divides $n^3 - n$". I have done so here to aid in my clear expression, but you should try to craft your argument without using phrases like:

1. "now let $k = n$"
2. "assume $P_n$"
3. "the theorem is true for $n$"

### 1.2.1 Class activities

**Activity 1.2.1**

**(a)** Show, using induction, that if $n$ is a natural number, then 3 divides $4^n - 1$.

Here $P_n$ is the empty statement and $Q_n$ is the statement "3 divides $4^n - 1$". The empty statement is indistinguishable from the logical constant True.

**Solution**. The base case is to show that 0 satisfies the conclusion of the statement. But $3 \cdot 0 = 0 = 4^0 - 1$, so the base case is done.

The inductive case is always phrased as a conditional. "*If* $n$ is a natural number that is in $A$, *then* $n+1$ is also in $A$." Let us prove this statement. We will use a direct proof, assuming the hypothesis (3 divides $4^n - 1$) and deducing the conclusion (3 divides $4^{n+1} - 1$).

Since 3 divides $4^n - 1$, the definition of divisibility tells us there is $k$ such that

$$3k = 4^n - 1.$$

Multiplying this equation by 4 and adding 3, we obtain

$$12k + 3 = 4(4^n - 1) + 3 = 4^{n+1} - 4 + 3 = 4^{n+1} - 1.$$

Since $12k + 3 = 3(4k+1)$, we have shown that $3 \cdot (4k+1) = 4^{n+1} - 1$ and the induction step is complete, as is the proof.

**Activity 1.2.2** Prove that for all natural numbers $n$, 6 divides $n^3 - n$. Use the induction framework.

**Hint**. The base case is $n = 0$ just like before. The inductive step is to prove: if 6 divides $n^3 - n$, it also divides $(n+1)^3 - (n+1)$.

Here are some helpful facts that you can use without proof. In a math class, we'd prove these as exercises as well, but here I'm hoping to provide enough math hints that you can focus more on the logical structure of the argument and less on the arithmetic.

1. If 3 divides $\ell$ and 2 divides $\ell$, then 6 divides $\ell$.
2. "$a$ is even" is the same statement as "2 divides $a$".
3. If $a$ divides $b$, then $a$ divides $kb$ for all integers $k$.
4. If $a$ divides $b$ and $a$ divides $c$, then $a$ divides $b \pm c$.

**Activity 1.2.3** In this activity we deal with points in the $n$-dimensional Euclidean space $\mathbb{R}^n$. Such a point is specified by an $n$-tuple of coordinates $(x_1, x_2, \ldots, x_n)$, where each $x_i \in \mathbb{R}$.

The *unit cube* in $\mathbb{R}^n$, or *unit n-cube*, is the subset $I^n$ of $\mathbb{R}^n$ defined by

$$I^n = \{(x_1, \ldots, x_n) \colon 0 \leq x_i \leq 1 \text{ for all } i\}.$$

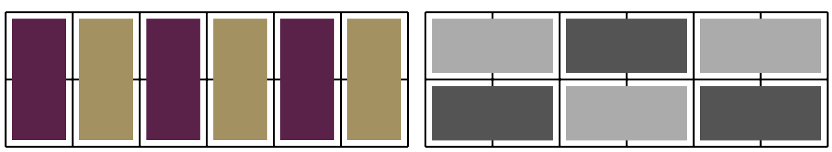
Just as a 3-dimensional cube has 2-, 1-, and 0-dimensional faces (usually called faces, edges, and corners, respectively), the $n$-cube has faces of all lower dimensions. We are interested in the corners.

The corners of $I^n$ are defined to be the points of $I^n$, all of whose coordinates are either 0 or 1. For example, $(0, 1, 1, 1, 0, 1, 0)$ is a corner of $I^7$.

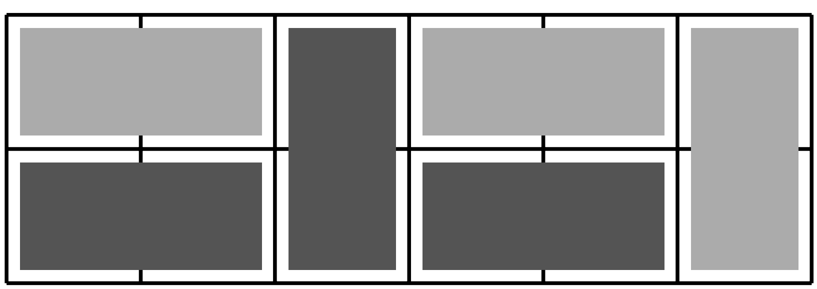
**(a)** Prove that $I^n$ has $2^n$ corners using the induction framework.

**Activity 1.2.4**

**(a)** Consider a rectangular $2 \times n$ array of squares, and the problem of determining the number of ways it may be tiled by $n$ dominoes. Each domino must cover exactly 2 adjacent squares, without overlaps. So, one way is to use all parallel dominoes. If $n$ happens to be even, all horizontal dominoes will work as well.



Of course, other tilings are also possible.



You can probably draw all 13 tilings of the $2 \times 6$ grid quite easily. It turns out that 13 is also the value of $F_7$, the 7th Fibonacci number. This isn't a coincidence, as you're asked to show below.

Using the recurrence relation above and the induction framework, show that there are $F_{n+1}$ such tilings of the $2 \times n$ array by dominoes, for all $n \geq 0$.

*Note.* For $n = 0$, we say that there is one way to tile an empty array with no dominoes. There would be zero ways to do it with more dominoes, and zero ways to tile a nonempty array with no dominoes.

**Hint**. Consider the ways in which a tiling of a $2 \times (n+2)$ array can arise from a smaller tiling. Remember, you need to show that the number of $(n+2)$-tilings is the sum of the number of $n$-tilings and the number of $(n+1)$-tilings.

**Answer**. If we look at the last two columns of an $(n+2)$-tiling, they have to either be both horizontal dominoes or both vertical. If they are both horizontal, removing both dominoes yields an $n$-tiling. If they are both vertical, removing the last one only yields an $(n+1)$-tiling.

**Activity 1.2.5** What is wrong with the following argument?

**Theorem 1.2.2 (Alleged theorem).** *All cars are blue.*

*Proof.* It is enough to show that given a nonempty finite set of cars, all of them are the same color. Since mine is blue, the result will follow at once. Let us prove by induction that every nonempty finite set of cars is monochromatic. If the set has just one car, it is surely monochromatic. Now let us suppose, by way of induction, that for some positive integer $n$ it has already been shown that every set of $n$ cars is monochromatic.

Consider a set $X$ of $n+1$ cars. We may form sets $Y_1$, $Y_2, \ldots, Y_{n+1}$ by deleting the $i$th car from $X$ to form $Y_i$. Applying the induction hypothesis to each of the sets $Y_i$ we see that each of these sets is monochromatic. But then $X$ is monochromatic as well, and the proof is complete. ■