09/05/2025: Multiple Proofs

CSCI 246: Discrete Structures

Textbook reference: Ch. 2, Hampkins

Quiz Set up

- **Guest lecturer Monday**: Paul Cornish.

Today's Agenda

- Weekly quiz (20 mins)
- Review ($\approx$ 10 mins)
- Group exercises ($\approx$ 10 mins)
- Review group exercises ($\approx$ 10 mins)

Weekly Quiz

1. *(Sec. 6 – Counterexample.)* Disprove the following conjecture: *Let a and b be integers. If $a|b$ and $b|a$, then $a = b$.*
2. *(Sec. 7 – Boolean Algebra.)* DeMorgan's laws are:

$$\neg(x \wedge y) = (\neg x) \vee (\neg y) \quad \text{and} \quad \neg(x \vee y) = (\neg x) \wedge (\neg y)$$

   Prove the first of these (using truth tables).
3. *(Sec. 7 – Boolean Algebra.)* Use DeMorgan's law to show how to disprove an if-and-only-if statement.

Reference Material: Scheinerman Definition 3.2

Let a and b be integers. We say a is *divisible* by b, written $b \mid a$, provided there is an integer c such that $bc = a$.

Notation reminder

$\neg$: `not` $\qquad$ $\vee$: `or` $\qquad$ $\wedge$: `and`

Intermezzo: Why are we doing all of this?

Objection. Why should computer scientists be concerned with formal structures (definitions, theorems, logic, etc.)?

Intermezzo: Why are we doing all of this?

Objection. Why should computer scientists be concerned with formal structures (definitions, theorems, logic, etc.)?

Example: Application of "Iff" to Cybsercurity. In security, "iff" statements are important because a one-way implication ("if") is not enough.

Intermezzo: Why are we doing all of this?

Objection. Why should computer scientists be concerned with formal structures (definitions, theorems, logic, etc.)?

Example: Application of "Iff" to Cybsercurity. In security, "iff" statements are important because a one-way implication ("if") is not enough. For example,

- *If a password is correct, then access is granted.* (Ok, but what if access is sometimes granted without a password?)

Intermezzo: Why are we doing all of this?

Objection. Why should computer scientists be concerned with formal structures (definitions, theorems, logic, etc.)?

Example: Application of "Iff" to Cybsercurity. In security, "iff" statements are important because a one-way implication ("if") is not enough. For example,

- *If a password is correct, then access is granted.* (Ok, but what if access is sometimes granted without a password?)
- The iff ensures no unintended backdoors or bypasses.

Intermezzo: Why are we doing all of this?

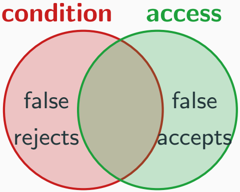
Objection. Why should computer scientists be concerned with formal structures (definitions, theorems, logic, etc.)?

Example: Application of "Iff" to Cybsercurity. In security, "iff" statements are important because a one-way implication ("if") is not enough. For example,

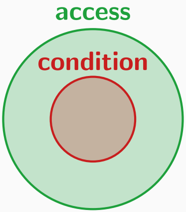
- *If a password is correct, then access is granted.* (Ok, but what if access is sometimes granted without a password?)
- The iff ensures no unintended backdoors or bypasses.

In general, the iff condition captures both **soundness** (no false accepts) and **completeness** (no false rejects).

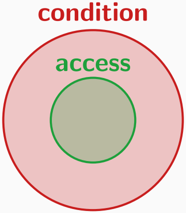
Soundness and Completeness of an Authentication System (Venn examples)



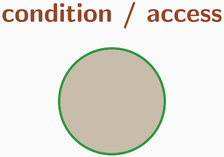
neither sound nor complete



complete (no false rejects) but not sound



sound (no false accepts) but not complete



sound and complete

Review additional group exercises from Boolean Algebra

Group work

Announcements about group work

- Ideas if you get stuck during group exercises:
  - (a) Get my/Paul's attention.
  - (b) Find other group to give a hint/lead.
  - (c) Use textbook as resource.
- It's okay to get stuck! That's a <u>natural</u> part of learning!

Quote of the Semester

"The best way to learn is to do; the worst way to teach is to talk."

– Paul Halmos, a renowned mathematician and expositor

Random group assignments

Aaron Christensen: 18
Aidan Sinclair: 6
Bennett Dijkstra: 15
Brendan Kelly: 4
Buggy Garza: 12
Cedric Jefferson: 14
Conner Brost: 2
Connor Graville: 7
David Knauert: 11
David Oswald: 10
Elias Martin: 4
Ericson O'Guinn: 6
Erik Halverson: 4
Francis Bush: 14
Garrett Miller: 3
George Cutler: 10
Georgia Franks: 13
Gregor Schmidt: 5

Hakyla Riggs: 15
Izayah Abayomi: 6
Jacob Ketola: 17
Jacob Ruiz: 9
Jaden Hampton: 9
Jeremy Ness: 2
Jonah Day: 8
Karter Gress: 1
Kyle Hoerner: 5
Landry Clarke: 17
Leon BirdHat: 13
Lillian Ziegler: 2
Matthew Rau: 16
Matyas Kari: 3
Micah Miller: 12
Michael Pitman: 7

Nathan Campbell: 7
Nathan Hooley: 10
Nicholas Rugani: 1
Noah Andersson: 8
Olivia Greuter: 13
Peter Van Vleet: 16
Pierce Dotson: 9
Quinn Carlson: 5
Ridley Christoferson: 15
Riley Smith: 12
Sierra Holleman: 1
Tanner Gramps: 16
Timothy True: 11
Titus Sykes: 14
Trey Randall: 3
William Grant: 11
William Sheldon: 8
Zachary Reller: 17

Group exercises

1. (Hamkins Ex. 2.1, first part) Prove that the sum, difference, and product of two even numbers is even.
2. (Hamkins Ex. 2.1, second part) Prove that the sum and difference of two odd numbers is even, but the product of two odd numbers is odd.

Solution to group exercise #1

Proposition. The sum, difference, and product of two even numbers is even.

Proof.

Annotation	**Main Text**
Convert Prop. to "if-then" form	We show that if x and y are even integers, then $x+y$, $x-y$, and xy are even.
State assumption ("if")	Let x and y be even integers
Unravel defs.	What goes here!?
*** The glue ***	
Unravel defs.	What goes here!?
State conclusion ("then")	Hence, $x+y, x-y$ and xy are even.

Solution to group exercise #1

Proposition. The sum, difference, and product of two even numbers is even.

Proof.

Annotation	Main Text
Convert Prop. to "if-then" form	We show that if x and y are even integers, then $x+y$, $x-y$, and xy are even.
State assumption ("if")	Let x and y be even integers
Unravel defs.	Then by the definition of even, there exist integers a, b such that $x = 2a$ and $y = 2b$.
*** The glue ***	What goes here?!?!
Unravel defs.	So there are integers c, d, e such that $x+y = 2c$, $x - y = 2d$, and $xy = 2e$.
State conclusion ("then")	Hence, $x+y, x-y$ and xy are even.

Solution to group exercise #1

Proposition. The sum, difference, and product of two even numbers is even.

Proof.

Annotation	Main Text
Convert Prop. to "if-then" form	We show that if x and y are even integers, then $x+y$, $x-y$, and xy are even.
State assumption ("if")	Let x and y be even integers
Unravel defs.	Then by the definition of even, there exist integers a, b such that $x = 2a$ and $y = 2b$.
*** The glue ***	We have: $$x+y = 2a+2b = 2\underbrace{(a+b)}_{:=c}$$ $$x-y = 2a-2b = 2\underbrace{(a-b)}_{:=d}$$ $$xy = 2a \cdot 2b = 2\underbrace{(2ab)}_{:=e}$$
Unravel defs.	So there are integers c, d, e such that $x+y = 2c$, $x-y = 2d$, and $xy = 2e$.
State conclusion ("then")	Hence, $x+y, x-y$ and xy are even.

Solution to group exercise #2

Proposition. The sum and difference of two odd numbers is even, but the product of odd numbers is odd.

Proof.

Annotation	**Main Text**
Convert Prop. to "if-then"	We show that if x and y are odd integers, then $x + y$ and $x - y$ are even, but xy is odd.
State "if"	Let x and y be odd integers.
Unravel defs.	What goes here?!?!
*** The glue ***	
Unravel defs.	What goes here?!?!
State "then"	Hence, $x + y$ and $x - y$ are even, but xy is odd.

Solution to group exercise #2

Proposition. The sum and difference of two odd numbers is even, but the product of odd numbers is odd.

Proof.

Annotation	Main Text
Convert Prop. to "if-then"	We show that if x and y are odd integers, then $x+y$ and $x-y$ are even, but xy is odd.
State "if"	Let x and y be odd integers.
Unravel defs.	Then by the definition of odd, there exist integers a, b such that $x = 2a+1$ and $y = 2b+1$.
*** The glue ***	What goes here?!?!
Unravel defs.	So there are integers c, d, e such that $x+y = 2c$, $x-y = 2d$, and $xy = 2e+1$.
State "then"	Hence, $x+y$ and $x-y$ are even, but xy is odd.

Solution to group exercise #2

Proposition. The sum and difference of two odd numbers is even, but the product of odd numbers is odd.

Proof.

Annotation	Main Text
Convert Prop. to "if-then"	We show that if x and y are odd integers, then $x+y$ and $x-y$ are even, but xy is odd.
State "if"	Let x and y be odd integers.
Unravel defs.	Then by the definition of odd, there exist integers a, b such that $x = 2a+1$ and $y = 2b+1$.
* The glue *	We have: $x + y = (2a+1) + (2b+1) = 2a + 2b + 2 = 2\underbrace{(a+b+1)}_{:=c}$ $x - y = (2a+1) - (2b+1) = 2a - 2b = 2\underbrace{(a-b)}_{:=d}$ $xy = (2a+1)(2b+1) = 4ab + 2a + 2b + 1 = 2\underbrace{(2ab+a+b)}_{:=e} + 1$
Unravel defs.	So there are integers c, d, e such that $x+y = 2c$, $x-y = 2d$, and $xy = 2e+1$.
State "then"	Hence, $x+y$ and $x-y$ are even, but xy is odd.