Logic

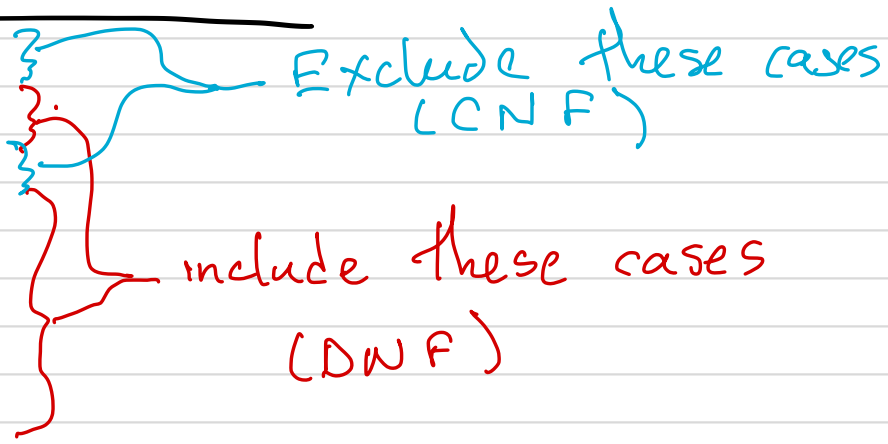
"Cogito, ergo sum!"
- Descartes

John Rachlin
discrete structures
Northeastern.

DNF vs. CNF

Creating a logical formula from truth table.

a	b	c	???
F	F	F	F
F	F	T	T
F	T	F	F
F	T	T	T
T	F	F	T
T	F	T	T
T	T	F	T
T	T	T	T



$(\neg a \wedge \neg b \wedge c) \vee (\neg a \wedge b \wedge c) \vee (a \wedge \neg b \wedge \neg c) \vee (a \wedge \neg b \wedge c)$

$\vee (a \wedge b \wedge \neg c) \vee (a \wedge b \wedge c)$

"Disjuctive Normal Form" (DNF):

$(x_1 \wedge x_2 \wedge \ldots) \vee (y_1 \wedge y_2 \wedge \ldots) \vee (\ldots)$

Alternatively, we focus on the false entries. The formula (whatever it is) is true when $\neg(\neg a \wedge \neg b \wedge \neg c) \wedge \neg(\neg a \wedge b \wedge \neg c)$

De Morgan's: $\neg(p \wedge q) \equiv \neg p \vee \neg q$

So: $\neg(\neg a \wedge \neg b \wedge \neg c) \equiv a \vee b \vee c$

$\neg(\neg a \wedge b \wedge \neg c) \equiv a \vee \neg b \vee c$

$(a \vee b \vee c) \wedge (a \vee \neg b \vee c)$

"Conjunctive Normal Form" (CNF):

$(x_1 \vee x_2 \vee \ldots) \wedge (y_1 \vee y_2 \vee \ldots) \wedge (\ldots)$

$$(a \vee b \vee c) \wedge (a \vee \neg b \vee c)$$

This is easier to simplify:

$$(a \vee c) \vee (b \wedge \neg b)$$

$$(a \vee c) \vee F$$

$$a \vee c$$

Watch For These simplifying opportunities:

DNF ... $(p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r)$ ...

$(p \wedge q) \wedge (r \vee \neg r)$ distributive

$(p \wedge q) \wedge T$ complement

$(p \wedge q)$ Identity

CNF ... $(p \vee q \vee r) \wedge (p \vee q \vee \neg r)$ ...

$(p \vee q) \vee (r \wedge \neg r)$ Distributive

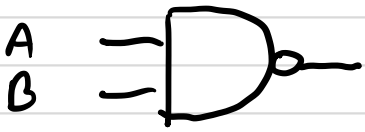
$(p \vee q) \vee F$ complement

$(p \vee q)$ Identity

0 = F , 1 = T

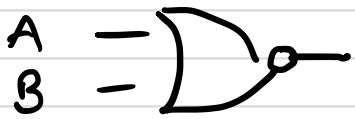
Logic Gates

$A \wedge B$ AND

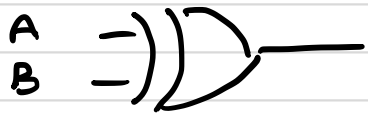


NAND

$A \vee B$ OR



NOR



XOR

XNOR

$\neg A$ NOT

"Not both A and B"

"A or B or Both"

"neither A nor B"

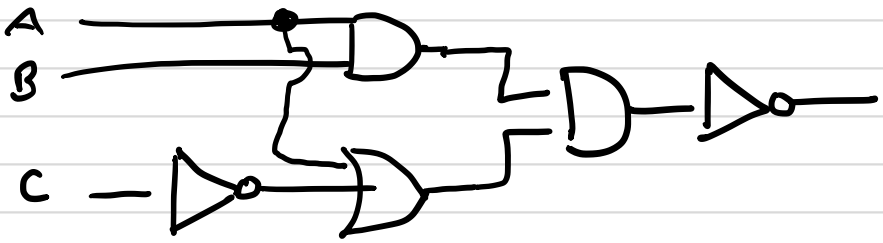
"A or B but not both"

"Neither A nor B" or both A and B (Truth values are same)

NOT AND NAND OR NOR XOR XNOR

A	B	$\neg A$	$A \wedge B$	$\neg(A \wedge B)$	$A \vee B$	$\neg(A \vee B)$	$A \oplus B$	$A \leftrightarrow B$
0	0	1	0	1	0	1	0	1
0	1	1	0	1	1	0	1	0
1	0	0	0	1	1	0	1	0
1	1	0	1	0	1	0	0	1

Simplifying a circuit

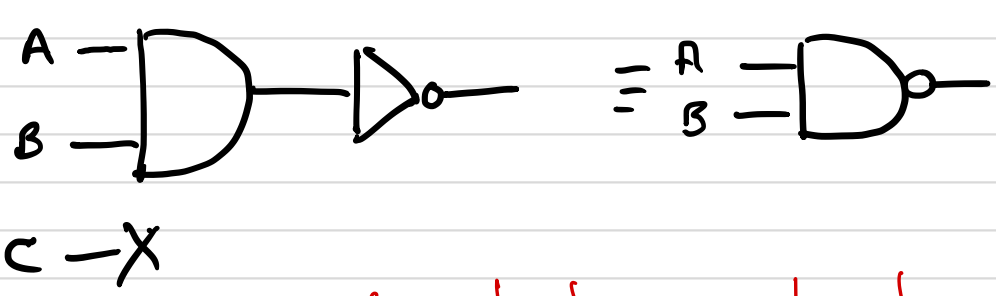


$\neg((A \wedge B) \wedge (A \vee \neg C))$

$\neg((A \wedge B \wedge A) \vee (A \wedge B \wedge \neg C))$ Distributive

$\neg((A \wedge B) \vee (A \wedge B \wedge \neg C))$ $A \wedge A \equiv A$

$\neg(A \wedge B)$ Absorption



A single Nand!

Its hot and humid

OR

Its hot ? humid : sunny

⇓

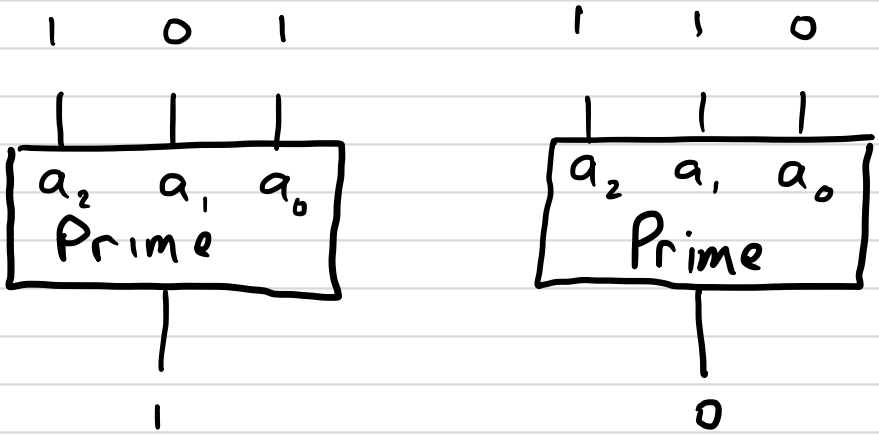
Its hot and humid

Designing a circuit - An example

Suppose 3 inputs a_2 a_1 a_0

which we interpret as an unsigned binary #

000... 111 or 0 to 7.



Circuit outputs 1 if the input binary (3-bits max) is Prime.

Prime #s: 2, 3, 5, 7, 11, 13, 17, 19, ...

3-bit range.

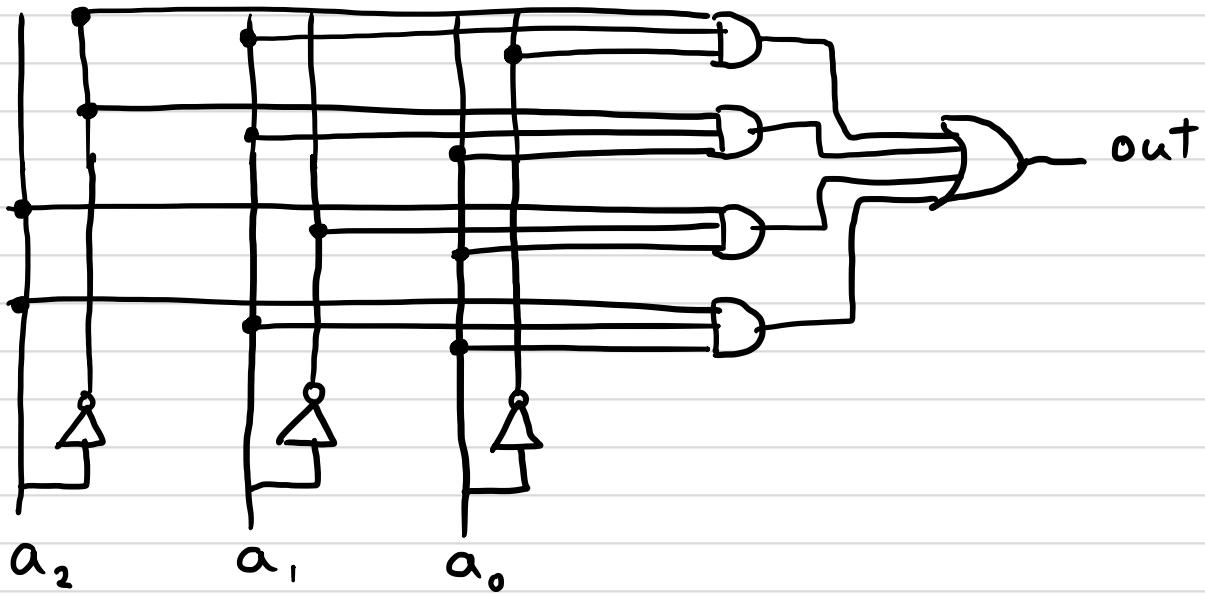
Note:
- A prime # is a whole # >1 whose factors are 1 and itself.
- By convention, 1 is <u>not</u> prime.
- Numbers with more than two factors are "composite"
- Largest known prime has 23 million digits
- RSA Encryption.

Build a truth table

a_2	a_1	a_0	out
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

DNF :

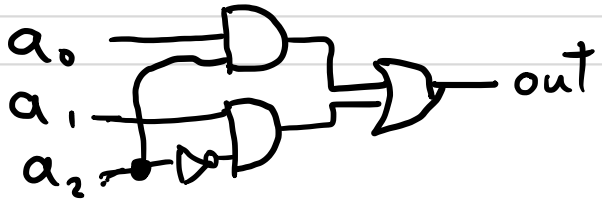
$$(\neg a_2 \wedge a_1 \wedge \neg a_0) \vee (\neg a_2 \wedge a_1 \wedge a_0) \vee (a_2 \wedge \neg a_1 \wedge a_0) \vee (a_2 \wedge a_1 \wedge a_0)$$



$$\left[(\neg a_2 \wedge a_1) \wedge (\neg a_0 \vee a_0)\right] \vee \left[(a_2 \wedge a_0) \wedge (\neg a_1 \vee a_1)\right]$$

$$((\neg a_2 \wedge a_1) \wedge T) \vee ((a_2 \wedge a_0) \wedge T)$$

$$(\neg a_2 \wedge a_1) \vee (a_2 \wedge a_0)$$



The limits of propositional logic

Aristotle offered the following "syllogism" (a type of logical argument).

All men are mortal
Socrates is a man
Therefore Socrates is mortal.

1st statement:

$(x \text{ is a man}) \rightarrow (x \text{ is mortal})$

But "x is a man" has no inherent truth value. It's true for some x's and false for other.

First Order Logic : claims about objects

We have:

- variables representing particular objects
  x = "Socrates"
- predicates establish claims about those objects.
  Human(Socrates) is true
  Human(Socrates) → Mortal(Socrates)

$\forall x$: The universal Quantifier

"For all x" : $a \wedge b \wedge c \wedge \ldots$

$\forall x$ Human$(x) \rightarrow$ Mortal(x)

Must be true for <u>all</u> objects, x.

For example:

$\forall x$ Prime$(x) \rightarrow$ Odd(x)

False: $x = 2$ (one counter example is enough!)

$\exists x$: the existential Quantifier.

"there exists <u>an</u> x" $a \vee b \vee c \ldots$

$\exists x$ NEU_Professor$(x) \wedge$ TeachesCS1800(x)

Must be true for <u>one or more</u> objects

Negating $\forall x$

$\neg \forall x\, P(x) \equiv \exists x\, \neg P(x)$

$\neg [\forall x\ \text{Prime}(x) \rightarrow \text{Odd}(x)]$

$\exists x\ \neg (\text{Prime}(x) \rightarrow \text{Odd}(x))$

$\exists x\ \neg (\neg \text{Prime}(x) \vee \text{Odd}(x))$

$\exists x\ \text{Prime}(x) \wedge \neg \text{Odd}(x)$ (True: $x = 2$)

Negating $\exists x$

$\neg \exists x\, P(x) \equiv \forall x\, \neg P(x)$

$\neg \exists x\ \text{Unicorn}(x) \equiv \forall x\ \neg \text{Unicorn}(x)$

Qualifying our range of objects

$\forall x \in \mathbb{N} : x + x = 2x$

$\exists y \in \mathbb{R} : y \notin \mathbb{Q}$ (Some Real #'s aren't rational)

Multi-argument Predicates

$$\forall x \forall y \forall z \ (\text{Mother}(x,y) \wedge \text{Mother}(y,z) \Rightarrow \text{Grandma}(x,z))$$

$\exists x \forall y \quad xy = 0 \qquad (\text{True}, x = 0)$

read: There is an x which, for all possible y values, $x \cdot y = 0$

Proof by example.

$\exists x \forall y \quad x + y = 0$

False. We set the value of x first and ask, is statement true? No, we can always find a counter example.

$\forall y \exists x \quad x + y = 0$

True. We imagine trying all possible values of y and, for each y seeing if we can find an x ☺

Proof by construction.

Logic and Proof

Last time we introduced quantifiers.

$\forall x$: for all x / for every x

$\exists x$: there exists an x / there is an x.

We gave some examples with multiple quantifiers, and we noted that the order of the quantifiers might matter.

$\forall x \in \text{locks}\ \exists y \in \text{keys}$: y opens x

"Every lock has a key that opens it."

$\exists y \in \text{keys}\ \forall x \in \text{locks}$: y opens x.

"There is a key that opens all locks"

The 2nd is a very different statement!

Similarly:

$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$: $y^3 = x$

"Every real # x has a cubed root: $y = \sqrt[3]{x}$" (TRUE)

$\exists y \in \mathbb{R}, \forall x \in \mathbb{R}$: $y^3 = x$

"There is a particular # y such that $y^3 = x$ for every real # x." (FALSE)

Introduction to Proofs

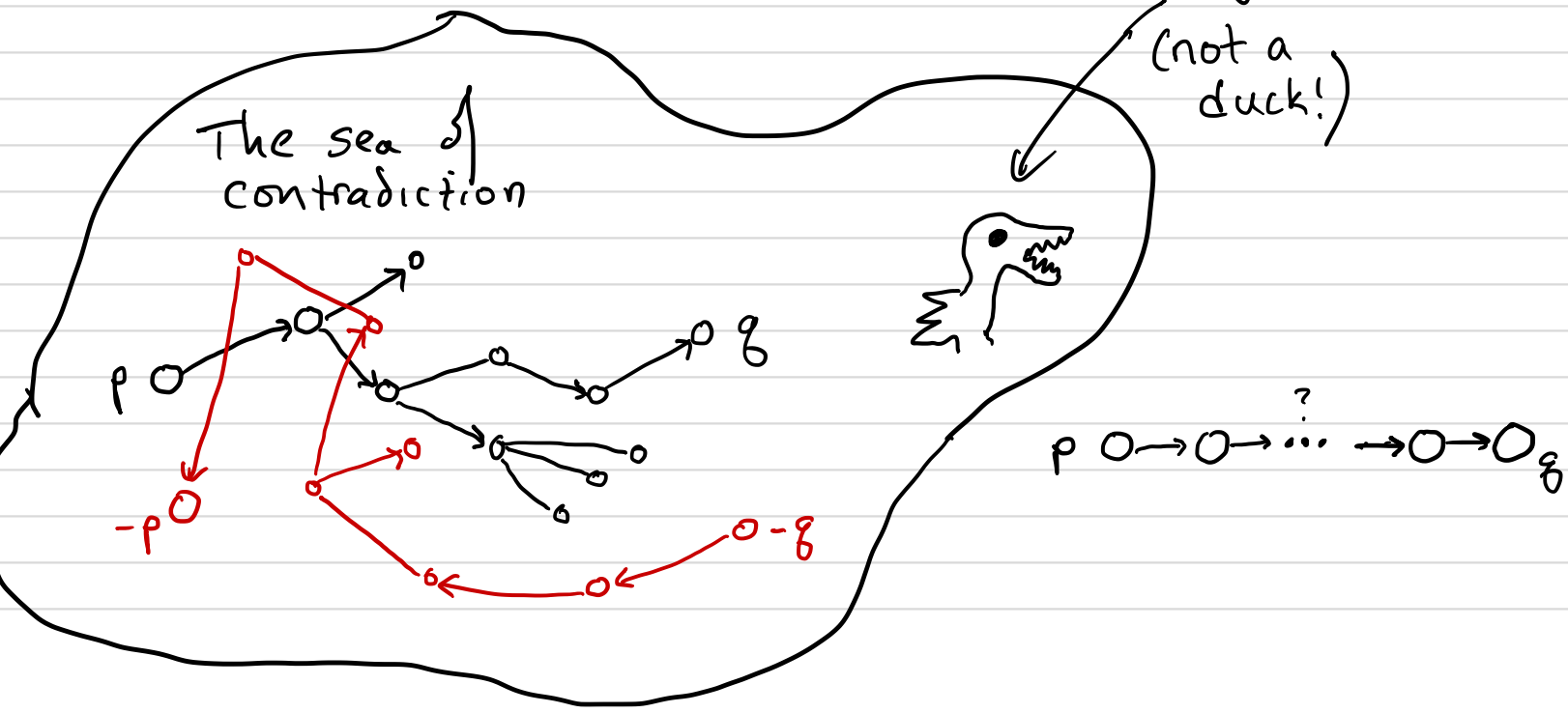
I think of mathematics as this vast (truly infinite) network of interconnected ideas. A proof is like finding a path from one idea to the next.

"if p then q"

"if and only if"

Often the path is not obvious and we must find intermediate steps along the way.

These statements are like islands of truth amid a sea of contradiction. The bridges are built from definitions, axioms, and other theorems.



Christian Goldbach
b. 1690 Konigsberg
d. 1764 Moscow

Statements

A statement is a sentence or mathematical expression that is definitely true or false.

True	False	Unknown
$2 \in \mathbb{Z}$	$2+2=5$	Goldbach's Conjecture
$\sqrt{2} \notin \mathbb{Z}$	3 is even	
Prime(13)	$\forall x \in \mathbb{N}$: even(x)	$P = NP$

Not a statement / "Open Statement"

$x > 5$: x is greater than 5.

Prime(x) : The number x is prime.

} which x?

Example: $\forall a,b,c,n \in \mathbb{N}, n>2 : a^n + b^n \neq c^n$

"Fermat's Last Theorem"

Fermat : 1607 - 1665

Proved by British Mathematician Andrew Wiles (1994)

1993: "Modular Forms, Elliptic Curves, and Galois Representations"

Goldbach's Conjecture: Every even integer greater than 2 is the sum of two prime numbers.

P: set of prime #s

S: even integers > 2 $\{x : x > 2, \text{even}(x)\}$

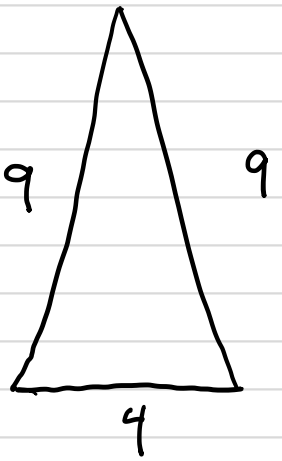
$(n \in S) \rightarrow (\exists p,q \in P, n = p+q)$

$\forall n \in S \; \exists p,q \in P : n = p+q$

Unproven but widely believed to be true

The Scarecrow's new Brain

"The sum of the square roots of any two sides of an isosceles triangle is equal to the square root of the remaining side."



$\sqrt{9} + \sqrt{9} = \sqrt{4}$ (No)

$\sqrt{9} + \sqrt{4} = \sqrt{9}$ (No)

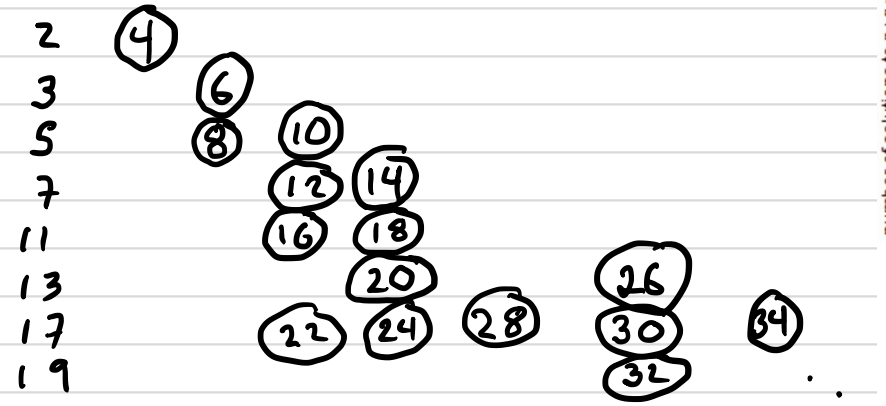
Umm .... this mathematical statement would be FALSE!

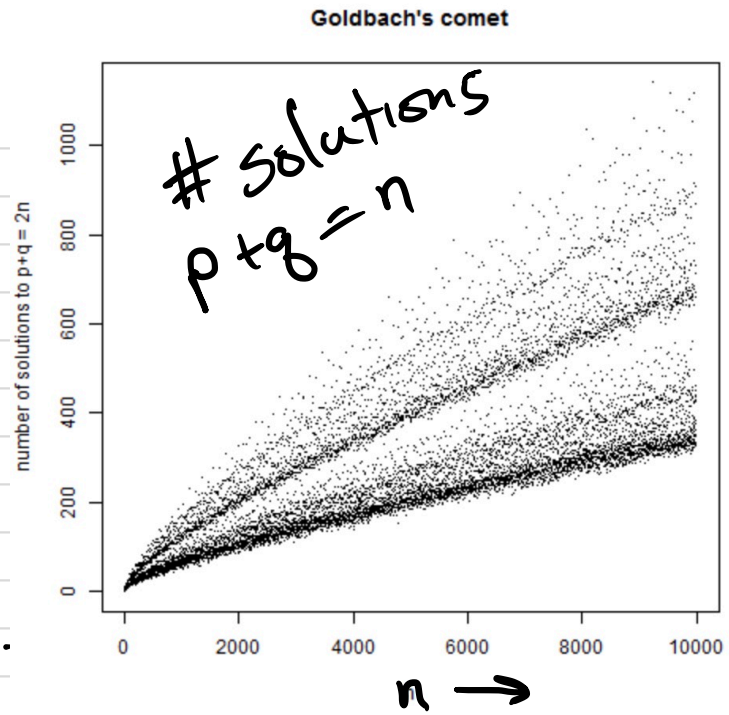
https://www.youtube.com/watch?v=1Xpb_9fhoBM

$100 = 3 + 97 \quad 41 + 59$
$11 + 89 \quad 47 + 53$
$17 + 83$
$29 + 71$

Consider:

2 3 5 7 11 13 17





solutions $p+q=n$

Proofs with Quantifiers: $\forall x$

- $\forall x \in Even : x^2 \in Even$

False approach: picking a specific value of x doesn't prove the "for all"

$x = 4 \Rightarrow x^2 = 16 \quad \therefore x^2$ is even.

Correct Approach: Suppose x is an (arbitrarily chosen) even integer.

Then $x = 2k$ for some $k \in \mathbb{Z}$ (Defn of even)

$x^2 = (2k)^2 = 4k^2 = 2m$

$(m = 2k^2)$

$\therefore x^2$ is even (Defn of even)

Prove: $\forall x \; Even(x) \rightarrow Even(x^2)$

Assume: $Even(x)$

Shows: $Even(x^2)$

} modus Ponens (Direct Proof)

Proof with Quantifiers: $\exists x$

It suffices to either give an example or show how to create it.

Prove: $\exists x \in \text{Even} : x \in \text{Prime}$ ← Even, Prime are sets

$\exists x : \text{Even}(x) \wedge \text{Prime}(x)$ ← Even & Prime are predicates.

2 is divisible by only 1 and itself

2 is Prime

$2 = 2 \cdot k \quad (k = 1)$

2 is Even

$\therefore$ 2 is an even Prime. ■

Prove: $\forall x \exists y \quad x + y = 1$

Choose: $y = 1 - x$ for any arbitrarily chosen x.

■

2nd-most

The worlds ∧ simplest proof?

The sum of two even integers is even.

Let x, y be two arbitrary even integers

Then $x = 2n$, $y = 2m$

So $x + y = 2n + 2m = 2(n+m) = 2k$.

where $k = n+m$

$\therefore$ $x+y$ is even. ∎

a) Prove sum of two odd integers is even.

b) Prove sum of even and odd is odd.

Logic and Proof

Direct Proof

> Proposition: $p \to q$
> Proof: Suppose p
> ⋮
> Therefore q. ■

Direct Proof Outline

Looking again at the truth table for $p \to q$:

p	q	$p \to q$	
F	F	T	} Implication is automatically true if p is false
F	T	T	
T	F	F	} Implication is true if q is also true and false if q is false.
T	T	T	

With direct proof we apply modus ponens repeatedly:

Suppose P.

$P \to U$
$U \to V$
$V \to W$
$W \to Q$

Therefore Q.

What would we derive if $p \to q$ is false?

$$p \wedge \neg(p \to q) \equiv p \wedge \neg(\neg p \vee q)$$
$$= p \wedge (p \wedge \neg q)$$
$$= p \wedge \neg q$$

So deriving $\neg q$ i.e, $p \wedge \neg q$ from assuming p <u>disproves</u> the implication. i.e, $\neg(p \to q)$ must be true.

Example

$$\forall x \in \mathbb{Z}\ \text{Odd}(x) \longleftrightarrow \text{Odd}(x^2+6x+8)$$

x is odd iff x^2+6x+8 is odd

We have to prove both: $\text{Odd}(x) \to \text{Odd}(x^2+6x+8)$
$\text{Odd}(x^2+6x+8) \to \text{Odd}(x)$

Suppose x is odd
$x = 2a+1$ (Defn of odd)

$$(2a+1)^2 + 6(2a+1) + 8$$
$$= 4a^2 + 4a + 1 + 12a + 6 + 8$$
$$= 4a^2 + 16a + 15 = 2(2a^2+8a+7) + 1$$
$$= 2m + 1$$
where $m = 2a^2+8a+7$

Therefore x^2+6x+8 is odd (Defn of odd)

■

Contrapositive

How to prove: If x^2+6x+8 is odd then x is odd.

We could do another direct proof, but a contrapositive proof is simpler.

Recall: $P \to Q \equiv \neg Q \to \neg P$

Proposition: $P \to Q$

Suppose: $\neg Q$

$\neg Q \to S$

$S \to T$

$T \to W$

$\vdots$

Therefore $\neg P$ ∎

Contrapositive Proof Outline

Contrapositive of if x^2+6x+8 is odd then x odd.

If x is not odd, then x^2+6x+8 is not odd.

$\Updownarrow$

if x is even, so is x^2+6x+8.

Suppose x is even

$x = 2a$ by definition

$(2a)^2 + 6(2a) + 8 = 4a^2 + 12a + 8$

$= 2(2a^2 + 6a + 4)$

$= 2b$ where $b = 2a^2+6a+4$

$\therefore$ x^2+6x+8 is even.

∎

Another contrapositive example. (with cases)

If 8 doesn't divide n^2-1, n is even.

Examples

n	n^2-1	Divides?
1	0	Yes
2	3	No
3	8	Yes
4	15	No
5	24	Yes
6	35	No
7	48	Yes
8	63	No
9	80	Yes
10	99	No
⋮	⋮	⋮

(Works for $n \leq 0$ too.)

What is the contrapositive?

"If n is odd, 8 does divide n^2-1"

Suppose n is odd.

$n = 2a+1$ Defn of odd.

$n^2-1 = (2a+1)^2 - 1 = 4a^2+4a$

$= 4a(a+1)$

a or $a+1$ is even.

i) a is even: $4 \cdot 2m(2m+1)$

$= 8m(2m+1)$

$= 8k \quad k = m(2m+1)$

So 8 evenly divides

ii) $a+1$ is even: $4a(a+1) = 4a(2m)$

$= 8am$

$= 8k \quad (k = a \cdot m)$

So 8 evenly divides. ■

Proof by Contradiction

Outline:

Proposition. P

Proof: Suppose $\neg P$

$\vdots$

Therefore $C \wedge \neg C$ ∎

P	C	$\neg P$	$C \wedge \neg C$	$\neg P \rightarrow (C \wedge \neg C)$
F	F	T	F	F
F	T	T	F	F
T	F	F	F	T
T	T	F	F	T

$\equiv$

$$P \equiv \neg P \rightarrow (C \wedge \neg C)$$

or $$(\neg P \rightarrow (C \wedge \neg C)) \rightarrow P \equiv T$$

IF: you can show that $\neg P$ leads to a contradiction, THEN you can conclude P

Believe Me! It's True!

Example.

$\forall a \in \mathbb{Z}$, if a^2 is even, a is even.

This is a claim about all integers.

What is the negation?

Suppose: $\neg \forall a \in \mathbb{Z}$ (a^2 is even $\rightarrow$ a is even)

$\exists a \in \mathbb{Z}$ $\quad \neg (a^2 \text{ is even} \rightarrow a \text{ is even})$

Defn. of Implication: $\exists a \in \mathbb{Z}$ $\quad \neg (\neg (a^2 \text{ is even}) \vee (a \text{ is even}))$

$\exists a \in \mathbb{Z}$ $\quad \neg\neg (a^2 \text{ is even}) \wedge \neg (a \text{ is even})$

$\exists a \in \mathbb{Z}$ $\quad a^2$ even $\wedge$ a is odd

Then $a^2 = (2c+1)^2 = 4c^2 + 4c + 1 = 2(2c^2+2c)+1$

$= 2k + 1$

$(k = 2c^2 + 2c)$

Therefore a^2 is odd.

So a^2 is both even and odd

(Contradiction)

Euclid: ≈ 300's BC

Prove: $\sqrt{2}$ irrational. (Euclid)

Defn. A real number x is rational if

$x = \frac{p}{q}$ for some $p, q \in \mathbb{Z}$

otherwise it is irrational.

We further assume <u>p and q have no common factors</u>, else they cancel out.

e.g $x = \frac{18}{4} = \frac{2 \cdot 9}{2 \cdot 2} = \frac{9}{2}$

Prove: $\sqrt{2}$ is irrational

Proof (By contradiction)

Assume: $\sqrt{2}$ is rational

$$\sqrt{2} = \frac{p}{q} \Rightarrow 2 = \frac{p^2}{q^2} \text{ or } p^2 = 2q^2$$

So p^2 is even, and so is p. (By our earlier proof.) i.e, $p = 2k$

$$2q^2 = p^2 = (2k)^2 = 4k^2$$

$q^2 = 2k^2 \Rightarrow q$ is also even!

So both p and q have a common factor (2) (Contradiction)

$\therefore \sqrt{2}$ is irrational.

Another Proof by Contradiction.

Prove: If $\overbrace{a \text{ is rational and } b \text{ is irrational}}^{P}$ then $\underbrace{a \cdot b \text{ is irrational.}}_{Q}$

$\neg(\neg P \vee Q)$

Suppose Not, ie, $\neg(P \to Q)$ or $P \wedge \neg Q$

Then there exists a, b such that a is rational, b is irrational and ab is rational.

Let $a = m/n \quad m, n \in \mathbb{Z}$ (Defn)

$ab = x/y \quad x, y \in \mathbb{Z}$ (Defn)

Then $ab = \frac{mb}{n} = \frac{x}{y}$ or $b = \frac{xn}{ym} = \frac{u}{v} \quad u, v \in \mathbb{Z}$

So b is rational and irrational (contradiction)

So $\neg(P \to Q)$ is impossible

Therefore: $P \to Q$

Prove: There are an infinite number of primes.

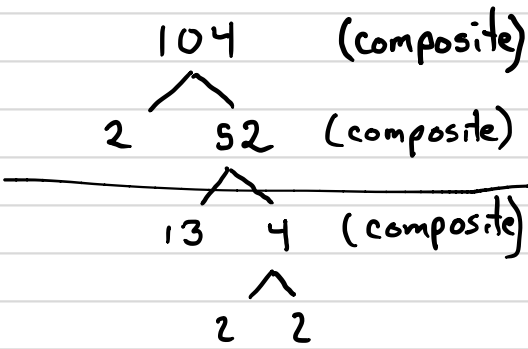
Note: Fundamental Theorem of Arithmetic:

Every integer greater than 1 is either prime or can be made from a unique product of prime factors.

$20 = 2 \times 2 \times 5$

$75 = 3 \times 5 \times 5$

etc.



Proof (by contradiction) of ∞ primes.

Suppose finite # primes

Then there is last prime, call it p.

$X = \underbrace{(2)(3)(5)(7)\cdots(p)}_{\text{The product of all primes}} =$

So each prime divides X evenly.

$X + 1 = (2)(3)(5)\cdots(p) + 1$

Is $X+1$ divisible by any prime?

No! For example, the next number that 2 divides into is $X+2$, the next number that 3 divides is $X+3$ etc.

So there are no prime factors.

So $X+1$ is prime. But $x+1 > p$

$\therefore$ p is not the last Prime number.