CSCI 2200
FOUNDATIONS OF COMPUTER SCIENCE

David Goldschmidt
goldsd3@rpi.edu
Fall 2022

TRUTH TABLES

We can summarize our logical connectors using a truth table

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \rightarrow q$
F	**F**	**T**	**F**	**F**	**T**
F	**T**	**T**	**F**	**T**	**T**
T	**F**	**F**	**F**	**T**	**F**
T	**T**	**F**	**T**	**T**	**T**

Use these logical connectors to form compound propositions

Construct a truth table for $(p \vee q) \rightarrow r$, then highlight the rows for which $(p \vee q) \rightarrow r$ is **T**

PROVING EQUIVALENCE

We can prove the equivalence of different statements by comparing their truth tables…

…or we can apply the rules shown to the right for manipulating logical connectors

Using the rules shown to the right, can you prove that $p \rightarrow q$ is equivalent to $\neg q \rightarrow \neg p$ (i.e., the *contrapositive*)

As a hint, start here

1. *Associative:* $(p \wedge q) \wedge r \overset{\text{eqv}}{\equiv} p \wedge (q \wedge r)$;
   $(p \vee q) \vee r \overset{\text{eqv}}{\equiv} p \vee (q \vee r)$.
2. *Commutative:* $p \wedge q \overset{\text{eqv}}{\equiv} q \wedge p$;
   $p \vee q \overset{\text{eqv}}{\equiv} q \vee p$.
3. *Negations:* $\neg(\neg p) \overset{\text{eqv}}{\equiv} p$;
   $\neg(p \wedge q) \overset{\text{eqv}}{\equiv} \neg p \vee \neg q$;
   $\neg(p \vee q) \overset{\text{eqv}}{\equiv} \neg p \wedge \neg q$.
4. *Distributive:* $p \vee (q \wedge r) \overset{\text{eqv}}{\equiv} (p \vee q) \wedge (p \vee r)$;
   $p \wedge (q \vee r) \overset{\text{eqv}}{\equiv} (p \wedge q) \vee (p \wedge r)$.
5. *Implication:* $p \rightarrow q \overset{\text{eqv}}{\equiv} \neg q \rightarrow \neg p$;
   $p \rightarrow q \overset{\text{eqv}}{\equiv} \neg p \vee q$.

PROVING EQUIVALENCE

Add $q \rightarrow p$ to the truth table…

…definitely not equivalent!

We can always use truth tables to determine logical equivalence…

…e.g., we can show the following propositions to be equivalent via truth tables

$$p \rightarrow q \overset{\text{eqv}}{\equiv} \neg p \vee q \overset{\text{eqv}}{\equiv} \neg q \rightarrow \neg p$$

p	q	$\neg p$	$\neg q$	$p \rightarrow q$	$\neg p \vee q$	$\neg q \rightarrow \neg p$
F	**F**	**T**	**T**	**T**	**T**	**T**
F	**T**	**T**	**F**	**T**	**T**	**T**
T	**F**	**F**	**T**	**F**	**F**	**F**
T	**T**	**F**	**F**	**T**	**T**	**T**

QUANTIFIERS

A *quantifier* describes "how many" objects in the set we are referring to

Propositions often contain quantifiers…

p: my cat has whiskers

q: all cats have whiskers

r: every map can be colored with four colors such that no adjacent regions are the same color

s: every integer $n > 2$ is the sum of two prime numbers (Goldbach, 1742)

t: there is a triple of integers (a, b, c) for which $a^2 + b^2 = c^2$

PREDICATES – FOR ALL

For proposition q, the quantifier <u>all</u> describes which cats we are talking about…

q: all cats have whiskers

Very precisely, we have set $C = \{ x \mid x \text{ is a cat} \}$

We also define *predicate* $P(x)$ = "cat x has whiskers"

To precisely claim that "all cats have whiskers," we write…

$$\forall x \in C : P(x)$$

Read this as "for all x in C, the statement $P(x)$ is true"—here, C is the *domain* of $P(x)$

PREDICATES – THERE EXISTS

For proposition u, what is the quantifier and what set does it describe?

u: there is a monster with tentacles and fangs

Very precisely, we have domain set $M = \{ m \mid m \text{ is a monster} \}$

We define predicate $Q(a)$ = "a has tentacles and fangs"

To precisely claim that "there is a monster with tentacles and fangs," we write…

$$\exists x \in M : Q(x)$$

Read this as "there exists an x in M for which statement $Q(x)$ is true"

COMPOUND PREDICATES

For proposition u, we could define multiple predicates

u: there is a monster with tentacles and fangs

We define predicate $G(a)$ = "a has tentacles"

And we define predicate $H(a)$ = "a has fangs"

Then we can write the claim using a *compound predicate*…

$$\exists x \in M : (G(x) \wedge H(x))$$

Read this as "there exists an x in M for which both $G(x)$ and $H(x)$ are true"

NEGATING QUANTIFIERS

What does the following negated proposition mean?

IT IS NOT THE CASE THAT(there is a monster with tentacles)

Define predicate $G(a)$ = "a has tentacles"

To precisely state the claim above, we write…

$$\neg(\exists x \in M : G(x))$$

NEGATING QUANTIFIERS

What does the following negated proposition mean?

IT IS NOT THE CASE THAT(there is a monster with tentacles)

Define predicate $G(a)$ = "a has tentacles"

To precisely state the claim above, we write…

$$\neg(\ \exists x \in M : G(x)\ ) \overset{\text{eqv}}{\equiv} \forall x \in M : \neg G(x)$$

Read this equivalence as "all monsters do not have tentacles"

NEGATING QUANTIFIERS

What does the following negated proposition mean?

IT IS NOT THE CASE THAT(all cats have whiskers)

Define predicate $P(x)$ = "cat x has whiskers"

To precisely state the claim above, we write…

$$\neg(\ \forall x \in C : P(x)\ ) \overset{\text{eqv}}{\equiv} \exists x \in C : \neg P(x)$$

Read this equivalence as "there exists a cat that does not have whiskers"

PROOFS WITH QUANTIFIERS

Claim 1: $\forall n > 2$ with $n \in \mathbb{N}$: if n is even, then n is the sum of two primes (Goldbach, 1742)

Claim 2: $\exists (a, b, c) \in \mathbb{N}^3 : a^2 + b^2 = c^2$

What would it take to prove each of these claims…?

Claim 3: $\neg\exists (a, b, c) \in \mathbb{N}^3 : a^3 + b^3 = c^3$

Claim 4: $\forall (a, b, c) \in \mathbb{N}^3 : a^3 + b^3 \neq c^3$

A DIRECT PROOF OF AN IMPLICATION

Given a claim in the form $p \rightarrow q$, we can consider using a *direct proof* as follows…

Proof. We prove the implication using a direct proof.

1. Start by assuming that the statement claimed in p is true
2. Restate your assumption in mathematical terms, as necessary
3. Use mathematical and logical derivations to relate your above assumptions to q
4. Argue that you have shown that q must be true
5. End by concluding that q is true ■

A DIRECT PROOF OF AN IMPLICATION – EXAMPLE

Prove the following claim: if $x, y \in \mathbb{Q}$, then $x + y \in \mathbb{Q}$

Proof. We prove the implication using a direct proof.

1. Assume that $x, y \in \mathbb{Q}$, i.e., x and y are rational.
2. Then, by definition, there are integers a, c and natural numbers b, d such that $x = a/b$ and $y = c/d$.
3. Then $x + y = (ad + bc)/bd$.
4. Since $ad + bc \in \mathbb{Z}$ and $bd \in \mathbb{N}$, $(ad + bc)/bd$ is rational (by definition).
5. Thus, we conclude from steps 3 and 4 that $x + y \in \mathbb{Q}$. ■

We made no assumptions about x…

…therefore, we proved $\forall x : P(x)$

PROVE USING A DIRECT PROOF…

Given $x \in \mathbb{R}$; claim $P(x)$: if $\underbrace{4^x - 1 \text{ is divisible by } 3}_{p}$, then $\underbrace{4^{x+1} - 1 \text{ is divisible by } 3}_{q}$

Proof. We prove the claim using a direct proof.

1. Assume that p is true, i.e., $4^x - 1$ is divisible by 3.
2. This means that $4^x - 1 = 3k$ for an integer k; from this, $4^x = 3k + 1$.
3. Since $4^{x+1} = 4 \cdot 4^x$, we have $4^{x+1} = 4 \cdot (3k + 1) = 12k + 4$.

   Therefore, $4^{x+1} - 1 = 12k + 3 = 3 \cdot (4k + 1)$, which is a multiple of 3.
4. Since $4^{x+1} - 1$ is a multiple of 3, we have shown that $4^{x+1} - 1$ is divisible by 3.
5. Therefore, the statement claimed in q is true. ■

A (TRICKY) PROBLEM TO WORK ON…

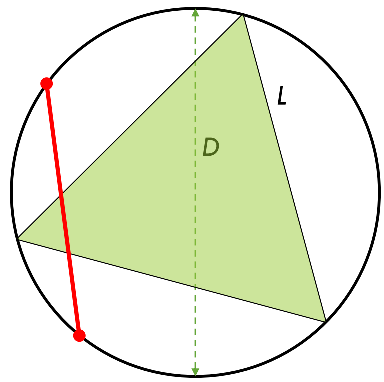
Can you solve this problem…
…by Tuesday's lecture?

Take any circle with diameter *D* and inscribe within it an equilateral triangle with side length *L*

Select a *chord* at random…

Recall that a chord is a line segment with its two endpoints on the circumference of the circle

What is the probability that the length of the chord is greater than *L*…?

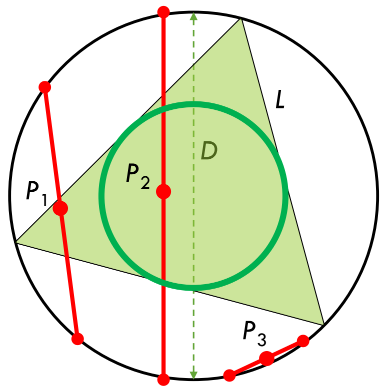


A (TRICKY) PROBLEM TO WORK ON – SOLUTION 1

Choose one point P randomly and uniformly within the circle and let point P be the midpoint of the chord

What is the probability that the length of the chord is greater than L…?

If point P falls within the green inner circle, the resulting chord will be greater than L (can you prove this?)



A (TRICKY) PROBLEM TO WORK ON – SOLUTION 1

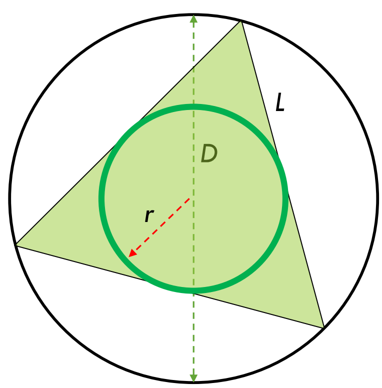
Choose one point P randomly and uniformly within the circle and let point P be the midpoint of the chord

What is the probability that the length of the chord is greater than L…?

If point P falls within the green inner circle, the resulting chord will be greater than L (can you prove this?)

Area of original circle: $\frac{1}{4}\pi D^2$

Area of inner circle: πr^2



With $r = \frac{1}{4}D$ (can you prove this?), the ratio of areas is ¼—therefore, the probability is ¼

A (TRICKY) PROBLEM TO WORK ON – SOLUTION 2

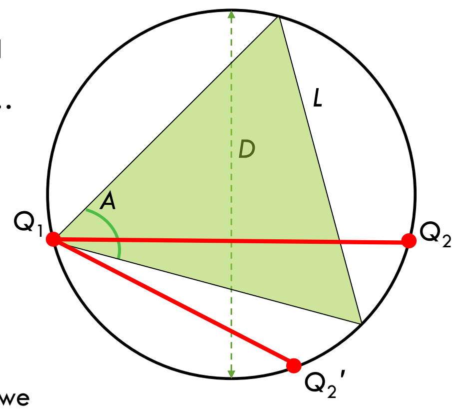
Define point Q_1 as one endpoint of the chord

Fix point Q_1 at any endpoint of the triangle…

…then randomly and uniformly select chord endpoint Q_2 anywhere on the circumference

If the chord falls "outside" of the triangle, then the chord length is not greater than *L*

If the chord is "within" the triangle, then the chord length is greater than *L*…



…given angle *A* is 60° out of 180° and that we can generalize Q_1 to be anywhere on the circumference, the probability that the length of the chord is greater than *L* is $^1/_3$

A (TRICKY) PROBLEM TO WORK ON – SOLUTION 3

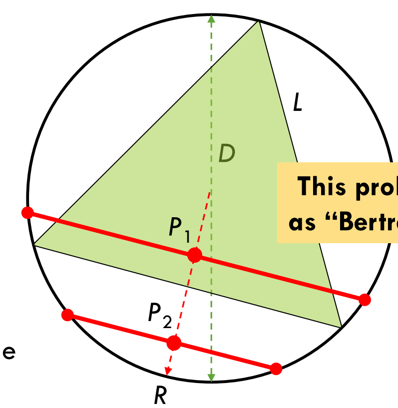
Focus on radius *R* of the given circle

Randomly and uniformly select point *P* anywhere along the radius…

…let point *P* be the midpoint of the chord

If point *P* is "close enough" to the center of the circle, then the chord length is greater than *L*; otherwise, it is not

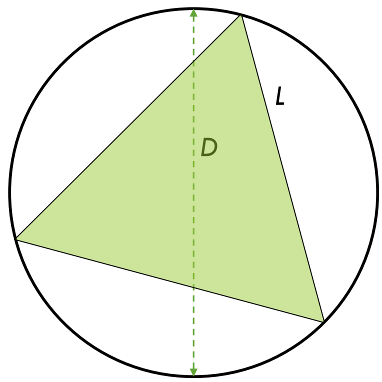
Also observe that the lower edge of the triangle bisects the radius (can you prove this?)



This problem is known as "Bertrand's paradox"

Given this—and the fact that we can generalize the radius and triangle to be anywhere around the circle—the probability is ½ due to the bisection

A (TRICKY) PROBLEM TO WORK ON – ???????????



Which solution is correct…?!

Important takeaways:

1. Do not prove anything until the claim or problem is precisely stated
2. Ask questions to complete step 1
3. Be creative—identify something true about the problem, then try to generalize
4. Strive to find a concise and elegant proof (but don't be discouraged if at first you don't succeed)

WHAT NEXT…?

Homework 1 is due by 11:59PM on Thursday, September 15

Create your team in Submitty in the Homework 1 Gradeable

- You at least need a team of one!

Recitation tomorrow (September 14) is a Q&A session to work on the homework

Get the textbook!

Email me extra-time accommodations ASAP