Summary.

First Rule of counting: Objects from a sequence of choices:
n_i possibilitities for ith choice : $n_1 \times n_2 \times \cdots \times n_k$ objects.

Second Rule of counting: If order does not matter.
Count with order: Divide number of orderings. Typically: $\binom{n}{k}$.

Stars and Bars: Sample k objects with replacement from n.
Order doesn't matter: Typically: $\binom{n+k-1}{n-1} = \binom{n+k-1}{k}$.

Inclusion/Exclusion: two sets of objects.
Add number of each subtract intersection of sets.
Sum Rule: If disjoint just add.

Combinatorial Proofs: Identity from counting same in two ways.
Pascal's Triangle Example: $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$.
RHS: Number of subsets of $n+1$ items size k.
LHS: $\binom{n}{k-1}$ counts subsets of $n+1$ items with first item.
$\binom{n}{k}$ counts subsets of $n+1$ items without first item.
Disjoint – so add!

Poll: How big is infinity?

Mark what's true.
(A) There are more real numbers than natural numbers.
(B) There are more rational numbers than natural numbers.
(C) There are more integers than natural numbers.
(D) pairs of natural numbers $>>$ natural numbers.

Same Size. Poll.

Two sets are the same size?

(A) Bijection between the sets.
(B) Count the objects and get the same number $\implies$ same size.
(C) Counting to infinity is hard.

(A), (B).
(C)?

Countable.

How to count?

0, 1, 2, 3, ...

The Counting numbers.
The natural numbers! $\mathbb{N}$

Definition:
S is **countable** if there is a bijection between S and some subset of $\mathbb{N}$.

If the subset of $\mathbb{N}$ is finite, S has finite **cardinality**.

If the subset of $\mathbb{N}$ is infinite, S is **countably infinite**.

Countably infinite subsets.

Enumerating a set implies countable.
Corollary: Any subset T of a countable set S is countable.

Enumerate T as follows:
Get next element, x, of S,
output only if $x \in T$.

Implications:
Z^+ is countable.
It is infinite since the list goes on.
There is a bijection with the natural numbers.
So it is countably infinite.

All countably infinite sets have the same cardinality.

Enumeration example.

All binary strings.
$B = \{0,1\}^*$.

$B = \{\phi, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, \ldots\}$.
ϕ is empty string.

For any string, it appears at some position in the list.
If n bits, it will appear before position 2^{n+1}.

Should be careful here.

$B = \{\phi; , 0, 00, 000, 0000, ...\}$
Never get to 1.

More fractions?

Enumerate the rational numbers in order...

$0, \ldots, 1/2, ..$

Where is $1/2$ in list?

After $1/3$, which is after $1/4$, which is after $1/5$...

A thing about fractions:
any two fractions has another fraction between it.

Can't even get to "next" fraction!

Can't list in "order".

Pairs of natural numbers.

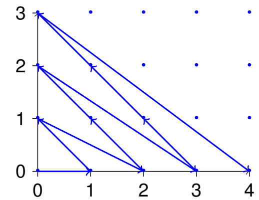
Consider pairs of natural numbers: $N \times N$
E.g.: $(1,2)$, $(100,30)$, etc.

For finite sets S_1 and S_2,
then $S_1 \times S_2$
has size $|S_1| \times |S_2|$.

So, $N \times N$ is countably infinite squared ???

Pairs of natural numbers.

Enumerate in list:
$(0,0),(1,0),(0,1),(2,0),(1,1),(0,2),\ldots\ldots$



The pair (a,b), is in first $\approx (a+b+1)(a+b)/2$ elements of list!
(i.e., "triangle").

Countably infinite.

Same size as the natural numbers!!

Poll.

Enumeration to get bijection with naturals?

(A) Integers: First all negatives, then positives.
(B) Integers: By absolute value, break ties however.
(C) Pairs of naturals: by sum of values, break ties however.
(D) Pairs of naturals: by value of first element.
(E) Pairs of integers: by sum of values, break ties.
(F) Pairs of integers: by sum of absolute values, break ties.

(B),(C), (F).

Rationals?

Positive rational number.
Lowest terms: a/b
$a, b \in N$
with $gcd(a,b) = 1$.

Infinite subset of $N \times N$.

Countably infinite!

All rational numbers?

Negative rationals are countable. (Same size as positive rationals.)

Put all rational numbers in a list.

First negative, then nonegative ??? No!

Repeatedly and alternatively take one from each list.
Interleave Streams in 61A

The rationals are countably infinite.

Real numbers..

Real numbers are same size as integers?

The reals.

Are the set of reals countable?

Lets consider the reals $[0,1]$.

Each real has a decimal representation.
.500000000... $(1/2)$
.785398162... $\pi/4$
.367879441... $1/e$
.632120558... $1-1/e$
.345212312... Some real number

Diagonalization.

If countable, there a listing, L contains all reals. For example

0: .500000000...
1: .785398162...
2: .367879441...
3: .632120558...
4: .345212312...
$\vdots$

Construct "diagonal" number: $.77677\ldots$

Diagonal Number: Digit i is 7 if number i's ith digit is not 7
and 6 otherwise.

Diagonal number for a list differs from every number in list!
Diagonal number not in list.

Diagonal number is real.

Contradiction!

Subset $[0,1]$ is not countable!!

All reals?

Subset $[0,1]$ is not countable!!

What about all reals?
No.

Any subset of a countable set is countable.

If reals are countable then so is $[0,1]$.

Diagonalization.

1. Assume that a set S can be enumerated.
2. Consider an arbitrary list of all the elements of S.
3. Use the diagonal from the list to construct a new element t.
4. Show that t is different from all elements in the list
   $\implies t$ is not in the list.
5. Show that t is in S.
6. Contradiction.

Another diagonalization.

The set of all subsets of N.

Example subsets of N: $\{0\}$, $\{0,\ldots,7\}$,
evens, odds, primes,

Assume is countable.

There is a listing, L, that contains all subsets of N.

Define a diagonal set, D:
If ith set in L does not contain i, $i \in D$.
otherwise $i \notin D$.

D is different from ith set in L for every i.
$\implies D$ is not in the listing.

D is a subset of N.

L does not contain all subsets of N.

Contradiction.

Theorem: The set of all subsets of N is not countable.
(The set of all subsets of S, is the **powerset** of N.)

Poll: diagonalization Proof.

Mark parts of proof.

(A) Integers are larger than naturals cuz obviously.
(B) Integers are countable cuz, interleaving bijection.
(C) Reals are uncountable cuz obviously!
(D) Reals can't be in a list: diagonal number not on list.
(E) Powerset in list: diagonal set not in list.

(B), (C)?, (D), (E)

The Continuum hypothesis.

There is no set with cardinality between the naturals and the reals.

First of Hilbert's problems!

Cardinalities of uncountable sets?

Cardinality of $[0,1]$ smaller than all the reals?

$f : R^+ \rightarrow [0,1]$.

$$f(x) = \begin{cases} x + \frac{1}{2} & 0 \leq x \leq 1/2 \\ \frac{1}{4x} & x > 1/2 \end{cases}$$

One to one. $x \neq y$
If both in $[0,1/2]$, a shift $\implies f(x) \neq f(y)$.
If neither in $[0,1/2]$ recipricoal $\implies f(x) \neq f(y)$.
If one is in $[0,1/2]$ and one isn't, different ranges $\implies f(x) \neq f(y)$.
Bijection!

$[0,1]$ is same cardinality as nonnegative reals!

Rao is freaked out.

Are real numbers even real?

Almost all real numbers can't be described.

π?
The ratio of the perimeter of a circle to its diameter.

e? Transendental number.
$\lim_{n\to\infty}(1+1/n)^n$.

$\sqrt{2}$? Algebraic number.
A solution of $x^2 = 2$.

Really, rationals seem fine for... say... calculus.

$\lim_{n\to\infty}\sum_{i=0}^{n}\frac{(b-a)}{n}f(x_i)$, where $x_i = a + i \times (b-a)/n$.

So why real numbers?

$\int_a^b f(x)dx$ is beautiful, succint notation
for a beautiful, succint, powerful idea.

What's the idea? Area. Width times Height.

Generalized Continuum hypothesis.

There is no infinite set whose cardinality is between the cardinality of an infinite set and its power set.

The powerset of a set is the set of all subsets.

Resolution of hypothesis?

Gödel. 1940.
Can't use math!
If math doesn't contain a contradiction.

This statement is a lie.

Is the statement above true?

The barber shaves every person who does not shave themselves.

Who shaves the barber?

Self reference.

Can a program refer to a program?

Can a program refer to itself?

Uh oh....

The Barber!

The barber shaves every person who does not shave themselves.

(A) Barber not Mark. Barber shaves Mark.
(B) Mark shaves the Barber.
(C) Barber doesn't shave themself.
(D) Barber shaves themself.

Its all true. It's all a problem.

Generalized Continuum hypothesis.

There is no infinite set whose cardinality is between the cardinality of an infinite set and its power set.

The powerset of a set is the set of all subsets.

Recall: powerset of the naturals is not countable.

Resolution of hypothesis?

Gödel. 1940.
Can't use math!
If math doesn't contain a contradiction.

This statement is a lie.

Is the statement above true?

The barber shaves every person who does not shave themselves.

Who shaves the barber?

Self reference.

Can a program refer to a program?

Can a program refer to itself?

Uh oh....

The reals.

Are the set of reals countable?

Lets consider the reals $[0, 1]$.

Each real has a decimal representation.
.500000000... $(1/2)$
.785398162... $\pi/4$
.367879441... $1/e$
.632120558... $1 - 1/e$
.345212312... Some real number

Diagonalization.

If countable, there a listing, L contains all reals. For example

0: .500000000...
1: .785398162...
2: .367879441...
3: .632120558...
4: .345212312...
$\vdots$

Construct "diagonal" number: $.77677\ldots$

Diagonal Number: Digit i is 7 if number i's ith digit is not 7
and 6 otherwise.

Diagonal number for a list differs from every number in list!
Diagonal number not in list.

Diagonal number is real.

Contradiction!

Subset $[0, 1]$ is not countable!!

All reals?

Subset $[0, 1]$ is not countable!!

What about all reals?
No.

Any subset of a countable set is countable.

If reals are countable then so is $[0, 1]$.

Diagonalization.

1. Assume that a set S can be enumerated.
2. Consider an arbitrary list of all the elements of S.
3. Use the diagonal from the list to construct a new element t.
4. Show that t is different from all elements in the list
   $\implies$ t is not in the list.
5. Show that t is in S.
6. Contradiction.

Another diagonalization.

The set of all subsets of N.

Example subsets of N: $\{0\}$, $\{0,\ldots,7\}$,
evens, odds, primes,

Assume is countable.

There is a listing, L, that contains all subsets of N.

Define a diagonal set, D:
If ith set in L does not contain i, $i \in D$.
otherwise $i \notin D$.

D is different from ith set in L for every i.
$\implies$ D is not in the listing.

D is a subset of N.

L does not contain all subsets of N.

Contradiction.

Theorem: The set of all subsets of N is not countable.
(The set of all subsets of S, is the **powerset** of N.)

Poll: diagonalization Proof.

Mark parts of proof.

(A) Integers are larger than naturals cuz obviously.
(B) Integers are countable cuz, interleaving bijection.
(C) Reals are uncountable cuz obviously!
(D) Reals can't be in a list: diagonal number not on list.
(E) Powerset in list: diagonal set not in list.

(B), (C)?, (D), (E)

Rao is freaked out.

Are real numbers even real?

Almost all real numbers can't be described.

π?
The ratio of the perimeter of a circle to its diameter.

e? Transcendental number.
$\lim_{n\to\infty}(1+1/n)^n$.

$\sqrt{2}$? Algebraic number.
A solution of $x^2 = 2$.

Really, rationals seem fine for... say... calculus.

$\lim_{n\to\infty}\sum_{i=0}^{n}\frac{(b-a)}{n}f(x_i)$, where $x_i = a + i \times (b-a)/n$.

So why real numbers?

$\int_a^b f(x)dx$ is beautiful, succint notation
for a beautiful, succint, powerful idea.

What's the idea? Area.

Generalized Continuum hypothesis.

There is no infinite set whose cardinality is between the cardinality of an infinite set and its power set.

The powerset of a set is the set of all subsets.

Resolution of hypothesis?

Gödel. 1940.
Can't use math!
If math doesn't contain a contradiction.

This statement is a lie.

Is the statement above true?

The barber shaves every person who does not shave themselves.

Who shaves the barber?

Self reference.

Can a program refer to a program?

Can a program refer to itself?

Uh oh....

The Barber!

The barber shaves every person who does not shave themselves.

(A) Barber not Mark. Barber shaves Mark.
(B) Mark shaves the Barber.
(C) Barber doesn't shave themself.
(D) Barber shaves themself.

Its all true. It's a problem.

Generalized Continuum hypothesis.

There is no infinite set whose cardinality is between the cardinality of an infinite set and its power set.

The powerset of a set is the set of all subsets.

Recall: powerset of the naturals is not countable.

Resolution of hypothesis?

Gödel. 1940.
Can't use math!
If math doesn't contain a contradiction.

This statement is a lie.

Is the statement above true?

The barber shaves every person who does not shave themselves.

Who shaves the barber?

Self reference.

Can a program refer to a program?

Can a program refer to itself?

Uh oh....

Changing Axioms?

Goedel:
Any set of axioms is either
inconsistent (can prove false statements) or
incomplete (true statements cannot be proven.)

Concrete example:
Continuum hypothesis: "no cardinatity between reals and naturals."
Continuum hypothesis not disprovable in ZFC
(Goedel 1940.)

Continuum hypothesis not provable.
(Cohen 1963: only Fields medal in logic)

BTW:
Cantor ..bipolar disorder..
Goedel ..starved himself out of fear of being poisoned..
Russell .. was fine.....but for ...two schizophrenic children..
Dangerous work?

See Logicomix by Doxiaidis, Papadimitriou (was professor here), Papadatos, Di Donna.

Is it actually useful?

Write me a program checker!

Check that the compiler works!

How about.. Check that the compiler terminates on a certain input.

$HALT(P, I)$
  P - program
  I - input.

Determines if $P(I)$ (P run on I) halts or loops forever.

Notice:
Need a computer
...with the notion of a stored program!!!!
(not an adding machine! not a person and an adding machine.)

Program is a text string.
Text string can be an input to a program.
Program can be an input to a program.

Implementing HALT.

$HALT(P, I)$
  P - program
  I - input.

Determines if $P(I)$ (P run on I) halts or loops forever.

Run P on I and check!

How long do you wait?

Something about infinity here, maybe?

Halt does not exist.

$HALT(P, I)$
  P - program
  I - input.

Determines if $P(I)$ (P run on I) halts or loops forever.

Theorem: There is no program HALT.

Proof: Yes! No! Yes! No! No! Yes! No! Yes! .. $\square$

Yes! No!...

What is he talking about?

(A) He is confused.
(B) Diagonalization.
(C) Welch-Berlekamp
(D) Professor is just strange.

(B) and (D) maybe? and maybe (A).

Professor does me some love Welch-Berlekamp though!

Programs?

What are programs?

(A) Instructions.
(B) Text.
(C) Binary String.
(D) They run on computers.

All are correct.

Halt and Turing.

Proof: Assume there is a program $HALT(\cdot,\cdot)$.

Turing(P)
1. If HALT(P,P) ="halts", then go into an infinite loop.
2. Otherwise, halt immediately.

Assumption: there is a program HALT.
There is text that "is" the program HALT.
There is text that is the program Turing.
Can run Turing on Turing!

Does Turing(Turing) halt?

Turing(Turing) halts
$\implies$ then HALTS(Turing, Turing) $=$ halts
$\implies$ Turing(Turing) loops forever.

Turing(Turing) loops forever
$\implies$ then HALTS(Turing, Turing) $\neq$ halts
$\implies$ Turing(Turing) halts.

Contradiction. Program HALT does not exist! □
Questions?

Proof play by play.

Assumed HALT(P, I) existed.

What is P? Text.
What is I? Text.

What does it mean to have a program HALT(P, I).
You have *Text* that is the program HALT(P, I).

Have Text that is the program TURING.
Here it is!!
from fancystuff import halt

Turing(P)
1. If HALT(P,P) ="halts", then go into an infinite loop.
2. Otherwise, halt immediately.

Turing "diagonalizes" on list of program.
It is not a program!!!!
$\implies$ HALT is not a program.

Questions?

Another view of proof: diagonalization.

Any program is a fixed length string.
Fixed length strings are enumerable.
Program halts or not on any input, which is a string.

	P_1	P_2	P_3	$\cdots$
P_1	H	H	L	$\cdots$
P_2	L	L	H	$\cdots$
P_3	L	H	H	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Halt - diagonal.
Turing - is not Halt.
and is different from every P_i on the diagonal.
Turing is not on list. Turing is not a program.
Turing can be constructed from Halt.
Halt does not exist! □

We are so smart!

Wow, that was easy!

We should be famous!

No computers for Turing!

In Turing's time.

No computers.

Adding machines.
e.g., Babbage (from table of logarithms) 1812.

Concept of program as data wasn't really there.

Turing machine.

A Turing machine.
– an (infinite) tape with characters
– be in a state, and read a character
– move left, right, and/or write a character.

Universal Turing machine
– an interpreter program for a Turing machine
– where the tape could be a description of a ... Turing machine!

Now that's a computer!

Turing: AI, self modifying code, learning...

Turing and computing.

Just a mathematician?

"Wrote" a chess program.

Simulated the program by hand to play chess.

It won! Once anyway.

Involved with computing labs through the 40s.

Helped Break the enigma code.
The polish machine...the *bomba.*

Computing on top of computing...

Computer, assembly code, programming language, browser, html, javascript..

We can't get enough of building more Turing machines.

Undecidable problems.

Does a program, P, print "Hello World"?
How? What is P? Text!!!!!!

Find exit points and add statement: **Print** "Hello World."

Can a set of notched tiles tile the infinite plane?
Proof: simulate a computer. Halts if finite.

Does a set of integer equations have a solution?
Example: " $x^n + y^n = 1$?"
Problem is undecidable.

Be careful!

Is there an integer solution to $x^n + y^n = 1$?
(Diophantine equation.)

The answer is yes or no. This "problem" is not undecidable.

Undecidability for Diophantine set of equations
$\Longrightarrow$ no program can take any set of integer equations and always corectly output whether it has an integer solution.

More about Alan Turing.

- Brilliant codebreaker during WWII, helped break German Enigma Code (which probably shortened war by 1 year).
- Seminal paper in numerical analysis: Condition number.
  Math 54 doesn't really work.
  Almost dependent matrices.
- Seminal paper in mathematical biology.
  Person: embryo is blob. Legs, arms, head.... How?
  Fly: blob. Torso becomes striped.
  Developed chemical reaction-diffusion networks that break symmetry.
- Imitation Game.

Turing: personal.

Tragic ending...

- Arrested as a homosexual, (not particularly closeted)
- given choice of prison or (quackish) injections to eliminate sex drive;
- took injections.
- lost security clearance...
- suffered from depression;
- (possibly) suicided with cyanide at age 42 in 1954.
  (A bite from the apple....) accident?
- British Government apologized (2009) and pardoned (2013).

Back to technical..

This statement is a lie. Neither true nor false!

Every person who doesn't shave themselves is shaved by the barber.

Who shaves the barber?

```
def Turing(P):
 if Halts(P,P): while(true): pass
 else:
  return
```

...Text of Halt...

Halt Progam $\implies$ Turing Program. ($P \implies Q$)

Turing("Turing")? Neither halts nor loops! $\implies$ No Turing program.

No Turing Program $\implies$ No halt program. ($\neg Q \implies \neg P$)

Program is text, so we can pass it to itself,
or refer to self.

Summary: decidability.

Computer Programs are an interesting thing.
Like Math.
Formal Systems.

Computer Programs cannot completely "understand" computer programs.

Computation is a lens for other action in the world.

Kolmogorov Complexity, Google, and CS70

Of strings, s.

Minimum sized program that prints string s.

What Kolmogorov complexity of a string of 1,000,000, one's?

What is Kolmogorov complexity of a string of n one's?

for $i = 1$ to n: print '1'.

Kolmogorov Complexity, Google, and CS70

What is the minimum I need to know (remember) to know stuff.

Radius of the earth? Distance to the sun? Population of the US? Acceleration due to gravity on earth?
Google. Plus reference.

Syntax of pandas? Google + Stackoverflow.
Plus "how to program" and remembering a bit.

What is π?
Kolmorogorov Complexity View:
perimeter of a circle/diameter.

What is e?
Kolmorogorov Complexity View(s):
Continuous Interest Rate: $(1 + r/n)^n \to e^r$.
Solution to: $dy/dx = y$,
$y \approx ((1+\frac{1}{n})^n)^x \to e^x$. Population growth. Covid.

Calculus: what is minimum you need to know?
Depends on your skills! Conceptualization.
Reason and understand an argument and you can generate a lot.

Calculus

What is the first half of calculus about?

The slope of a tangent line to a function at a point.

Slope is rise/run. Oh, yes: $\lim_{h\to 0} \frac{f(x+h)-f(x)}{h}$.

Chain rule? Derivative of a function composition.
Intuition: composition of two linear functions?
$f(x) = ax$, $g(x) = bx$. $f(g(x)) = ab\,x$. Slope is ab.
Multiply slopes!

$(f(g(x)))' = f'(\cdot)g'(\cdot)$

But...but...

For function slopes of tangent differ at different places.

So, where? $f(g(x))$
slope of f at $g(x)$ times slope of g at x.
$(f(g(x))' = f'(g(x))g'(x)$.

Product Rule.

Idea: use rise in function value!
$d(uv) = (u+du)(v+dv) - uv = udv + vdu + dudv \rightarrow udv + vdu$.
used foil.

Any concept:
A quick argument from basic concept of slope of a tangent line.

Perhaps.

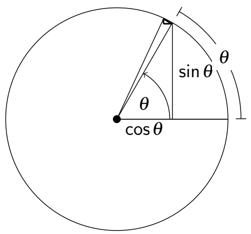
Derivative of sine?

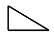
$\sin(x)$.

What is x? An angle in radians.

Let's call it θ and do derivative of $\sin\theta$.

θ - Length of arc of unit circle





Rise.
Similar triangle!!!
Rise proportional to cosine!

Fundamental Theorem of Calculus.

Conceptual: Height times Width = Area.

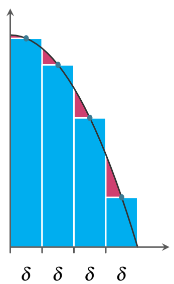
Useful?
Speed times Time is Distance.

Conceptual: Area is proportional to height.

If you change width, change in area is proportional to height.

Derivative (rate of change) of Area (Integral) under curve, is height of curve.

Calculus



Riemann Sum/Integral: $\int_a^b f(x)dx = lim_{\delta \rightarrow 0} \sum_i \delta f(a_i)$
"Area is defined as rectangles and add up some thin ones."

Derivative (Rate of change):
$F'(x) = \lim_{h \rightarrow 0} \frac{F(x+h)-F(x)}{h}$.
"Rise over run of close together points."

Fundamental Theorem: $F(b) - F(a) = \int_a^b F'(x)dx$.
"Area ($F(\cdot)$) under $f(x)$ grows at x, $F'(x)$, by $f(x)$"
Thus $F'(x) = f(x)$.

Arguments, reasoning.

What you know: slope, limit.
Plus: definition.
yields calculus.
Minimization, optimization, ...

Knowing how to program plus some syntax (google) gives the ability to program.

Knowing how to reason plus some definition gives calculus.

Discrete Math: basics are counting, how many, when are two sets the same size?

Probability: division.

...plus reasoning.

CS 70 : ideas.

Induction $\equiv$ every integer has a next one. Graph theory.
Number of edges is sum of degrees.
$\Delta + 1$ coloring. Neighbors only take up Δ.
Connectivity plus connected components.
Eulerian paths: if you enter you can leave.
Euler's formula: tree has $v-1$ edges and 1 face plus
each extra edge makes additional face.
$v - 1 + (f - 1) = e$

CS 70 : ideas.

Number theory.
A divisor of x and y divides $x-y$.
The remainder is always smaller than the divisor.
$\implies$ Euclid's GCD algorithm.
Multiplicative Inverse.
Fermat's theorem from function with inverse is a bijection.
Gives RSA.

Error Correction.
(Any) Two points determine a line.
(well, and d points determine a degree $d+1$-polynomials.
Cuz, factoring.
Find line by linear equations.
If a couple are wrong, then multiply them by zero, i.e., Error polynomial.

CS70 and your future?

What's going on?

Define. Understand properties. And build from there.

Tools: reasoning, proofs, care.

Gives power to your creativity and in your pursuits.

....and you will pursue probability in this course.