1: Communicating math

Math camp 2019

George Mason University

August 22, 2019

- Me: Arthur Dolgopolov,
- Don't hesitate to email me questions! Seriously.
  adolgopo@gmu.edu
- Lecture slides:
  https://arthurdolgopolov.net/teaching/mathcamp
- Wolfram Mathematica (free for students):
  https://cos.gmu.edu/mathematica/

- Calculus:

Vladimir Zorich Mathematical Analysis (Part I)

- Proofs, sets, logic:

Math for CS (chapters 3,4,8 + optionally 10,14,15)
https://courses.csail.mit.edu/6.042/spring17/mcs.pdf

- Linear algebra:

3Blue1Brown https://www.youtube.com/playlist?list=PLZHQObOWTQDPD3MizzM2xVFitgF8hE_ab

- Optimization:

Mathematical methods for economic theory Martin J. Osborne
https://mjo.osborne.economics.utoronto.ca/index.php/tutorial/index/1/toc

- Differential equations: ?, Macro I class handout, 3Blue1Brown, specialized textbooks,

Zhang, Wei-Bin. Differential equations, bifurcations, and chaos in economics. Vol. 68. World Scientific Publishing Company, 2005.

- 1. Set theory and notation;

- 1. Set theory and notation;
- Ultimate goal is to be able to count.

- 1. Set theory and notation;
- Ultimate goal is to be able to count.
- 2. Logic and propositions;

- 1. Set theory and notation;
- Ultimate goal is to be able to count.
- 2. Logic and propositions;
- 3. Proofs.

We are currently roughly at math level of the early XIX century (enough to get into MIT of the time). https://libraries.mit.edu/archives/exhibits/exam/algebra.html

Our ultimate goal is roughly year **1951** with optimality conditions.

Today we fill in the gap for set theory (Georg Cantor in **1874**), Boolean logic and order theory, all of them mostly from **XIX century**.

Math for CS (chapters 3,4,8 + optionally 10,14,15)
https://courses.csail.mit.edu/6.042/spring17/mcs.pdf

Mathematical methods for economic theory Martin J. Osborne (1.1: logic)
https://mjo.osborne.economics.utoronto.ca/index.php/tutorial/index/1/toc

Part 1: Logic

In English, we can modify, combine, and relate propositions with words such as "not," "and," "or," "implies," and "if-then." For example, we can combine three propositions into one like this:

If all *humans are mortal* **and all** *Greeks are human,* **then all** *Greeks are mortal.*

Propositional (Boolean) variables and propositions themselves, can take on only the values $T(true)$ and $F(false)$.

It is sometimes reasonable (and sometimes it is not) to use special notation:
$\neg, \wedge, \vee, \implies, \iff$
The order of operations is as above. Brackets work as usual. Or is not exclusive.

all *humans are mortal* $\wedge$ **all** *Greeks are human,* $\implies$ **all** *Greeks are mortal.*

NOT AND and *OR* combine propositions according to truth tables:

NOT ($\neg P$ or $\bar{P}$):

P	$\neg(P)$
T	F
F	T

(P OR Q):

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

(implies $P \implies Q$):

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

P implies Q,
Q follows from P,
Q is necessary for P,
P is sufficient for Q.

(implies $P \implies Q$):

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

$\implies$

An implication is true exactly when the if-part is false or the then-part is true.

P is sufficient condition for Q. Q is necessary condition for P.

Example from the book:

If Goldbach's Conjecture is true, then $x^2 \geq 0$ for every real number x.

$x > 100 \implies x > 10$ for all x

Seeing a unicorn implies seeing that aliens are real.

A predicate is a proposition whose truth depends on the value of variables.

$P(x) =$ *True* iff x is even
$P_{100}(x) =$ *True* iff $x > 100$
$P_{10}(x) =$ *True* iff $x > 100$
$P_{100}(x) \implies P_{10}(x) \forall x.$

(if and only if $P \iff Q$):

P	Q	$P \iff Q$
T	T	T
T	F	F
F	T	F
F	F	T

In other words

$\Longrightarrow$

An implication is true exactly when the if-part is false or the then-part is true.

(if and only if $P \iff Q$):

P	Q	$P \iff Q$
T	T	T
T	F	F
F	T	F
F	F	T

P is necessary and sufficient for Q,
P holds when Q holds and only then,
P if and only if Q,
P is equivalent to Q.
$P \implies Q$ and simultaneously $Q \implies P$ (prove it).

$(x^2 - 3x + 2 = 0) \iff (x = 1) \vee (x = 2)$

A	B	$A \vee ((\neg A) \wedge B)$	
T	T		
T	F		
F	T		
F	F		

Contrapositives:

If I am hungry, then I am grumpy.

$\iff$

If I am not grumpy, then I am not hungry.

Converse:

If I am grumpy, then I am hungry.

Converse is not equivalent to the proposition.

Proposition + Converse = IFF

If I am grumpy then I am hungry, and if I am hungry then I am grumpy

I am grumpy iff I am hungry

Quantifiers:
$\forall$: for all, universal
$\exists$: exists, for some, existential
$\in$: belongs to the set, is in
you can solve every problem we come up with, or, maybe, you can solve at least one problem we come up with.
$(Solve(x) \forall x \in P) \implies (\exists x \in P,\ s.t.\ Solve(x))$

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

For every even integer n greater than 2, there exist primes p and q such that $n = p + q$.

$\forall n \in \mathit{Evens}\ \exists p \in \mathit{Primes}\ \exists q \in \mathit{Primes},\ \text{s.t.}\ n = p + q$
Order of quantifiers matters!

Proofs:

Rule of inference, modus ponens

$((A = true) \wedge (A \implies B)) \implies B = true$

Law of excluded middle, tertium non datur, Whitehead, Russell (1962)

$A \vee (\neg A)$

Unlocks non-constructive proofs by contradiction at a cost of some complications.
A paradox: "This statement is false"

Practice: Obtain it from identity

Identity

$A \implies A$

Practice: Obtain double negation

Double negation

$\neg(\neg A) = A$

To explore the topic, browse through Metamath
http://us.metamath.org/mpegif/mmtheorems1.html.

Practice: use definitions of operators to prove these (from Zorich).

$$\neg(A \wedge B) \iff \neg A \vee \neg B$$
$$\neg(A \vee B) \iff \neg A \wedge \neg B$$
$$\neg(A \implies B) \iff A \wedge \neg B$$

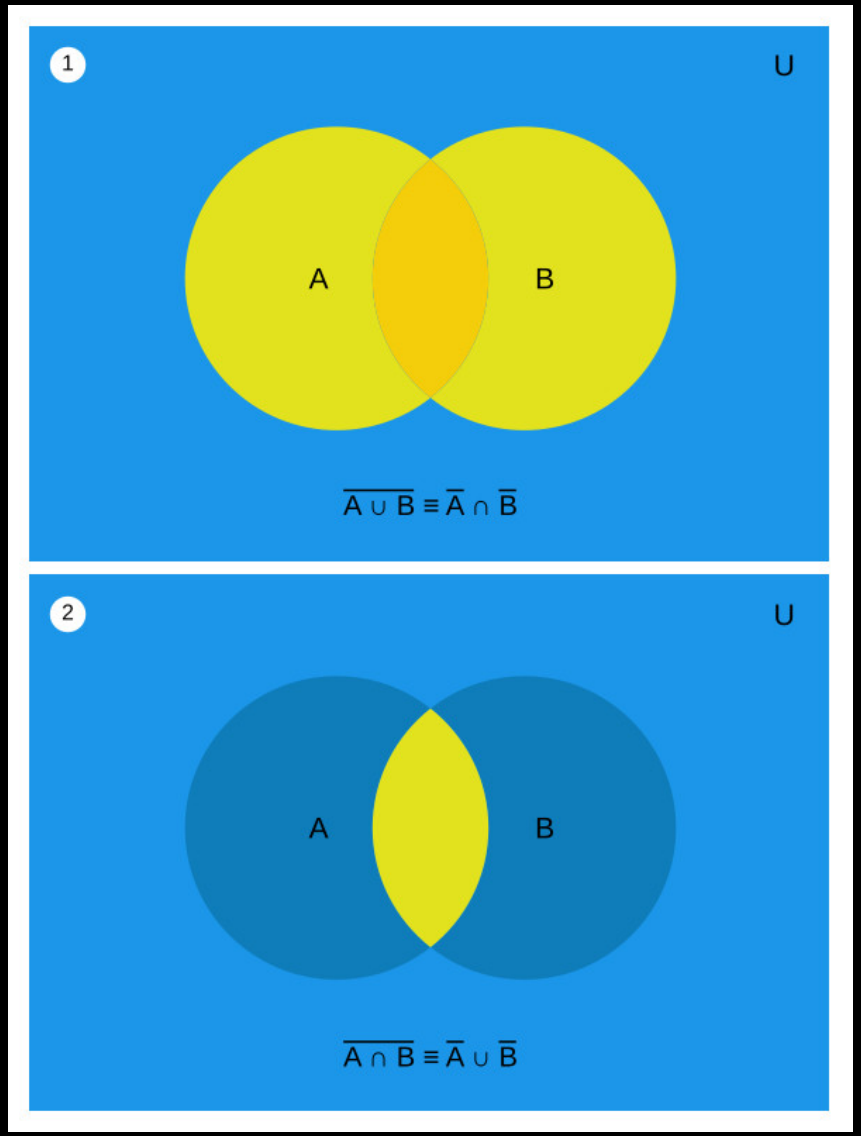


Figure: DeMorgan's Laws

- There is no one who likes being mocked.
- Everyone dislikes being mocked.

$$NOT(\exists x, \text{ s.t. } P(x)) \iff NOT(P(x))\forall x$$

- Algebraic structure on a set A is a collection of finitary operations on A; the set A with this structure is also called an **algebra**.

- Algebraic structure on a set A is a collection of finitary operations on A; the set A with this structure is also called an **algebra**.
- I.e. we need to define operations and "close" the space under

these operations. If we could have $A \wedge B =$,

- Algebraic structure on a set A is a collection of finitary operations on A; the set A with this structure is also called an **algebra**.
- I.e. we need to define operations and "close" the space under these operations. If we could have $A \wedge B =$  ,

- Algebraic structure on a set A is a collection of finitary operations on A; the set A with this structure is also called an **algebra**.
- I.e. we need to define operations and "close" the space under these operations. If we could have $A \wedge B =$  , set of propositions is not "closed" under $\wedge$.

- Algebraic structure on a set A is a collection of finitary operations on A; the set A with this structure is also called an **algebra**.
- I.e. we need to define operations and "close" the space under these operations. If we could have $A \wedge B =$  , set of propositions is not "closed" under $\wedge$.
- Our operations are $\neg, \wedge, \vee$, and our space is the space of propositions, closed under these operations, since propositional formulas are also propositions.

$A \wedge B \iff$

$$A \wedge B \iff B \wedge A \qquad \text{(AND is commutative)}$$

$$(A \wedge B) \wedge C \iff$$

$$A \wedge B \iff B \wedge A \qquad \text{(AND is commutative)}$$

$$(A \wedge B) \wedge C \iff A \wedge (B \wedge C) \qquad \text{(AND is associative)}$$

$$T \wedge A \iff$$

$$A \wedge B \iff B \wedge A \qquad \text{(AND is commutative)}$$

$$(A \wedge B) \wedge C \iff A \wedge (B \wedge C) \qquad \text{(AND is associative)}$$

$$T \wedge A \iff A \qquad \text{(identity)}$$

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

$$A \wedge B \iff B \wedge A \qquad \text{(AND is commutative)}$$

$$(A \wedge B) \wedge C \iff A \wedge (B \wedge C) \qquad \text{(AND is associative)}$$

$$T \wedge A \iff A \qquad \text{(identity)}$$

$$A \wedge (B \vee C) \iff (A \wedge B) \vee (A \wedge C) \qquad \text{(distributivity)}$$

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

$$A \wedge B \iff B \wedge A \qquad \text{(AND is commutative)}$$

$$(A \wedge B) \wedge C \iff A \wedge (B \wedge C) \qquad \text{(AND is associative)}$$

$$T \wedge A \iff A \qquad \text{(identity)}$$

$$A \wedge (B \vee C) \iff (A \wedge B) \vee (A \wedge C) \qquad \text{(distributivity)}$$

$$A \vee (B \wedge C) \iff (A \vee B) \wedge (A \vee C) \qquad \text{(distributivity)}$$

$$A \vee \bar{A} \iff$$

$$A \vee \bar{A} \iff T$$

$$F \wedge A \iff$$

$$A \vee \bar{A} \iff T$$

$$F \wedge A \iff F$$

$$A \wedge A \iff$$

$$A \vee \bar{A} \iff T$$

$$F \wedge A \iff F$$

$$A \wedge A \iff A$$

$$A \wedge \bar{A} \iff$$

$$A \vee \bar{A} \iff T$$

$$F \wedge A \iff F$$

$$A \wedge A \iff A$$

$$A \wedge \bar{A} \iff F$$

$$\neg\neg A \iff$$

$$A \vee \bar{A} \iff T$$

$$F \wedge A \iff F$$

$$A \wedge A \iff A$$

$$A \wedge \bar{A} \iff F$$

$$\neg\neg A \iff A$$

Part 2: Structures: Sets, Functions, Relations etc.

Cantor: "We take a set to be an assemblage of definite, perfectly distinguishable objects of our intuition or our thought into a coherent whole."

This is surprisingly not helpful.

What is a proper definition of set?

Cantor: "We take a set to be an assemblage of definite, perfectly distinguishable objects of our intuition or our thought into a coherent whole."

This is surprisingly not helpful.

What is a proper definition of set?

There isn't one.

Cantor: "We take a set to be an assemblage of definite, perfectly distinguishable objects of our intuition or our thought into a coherent whole."

This is surprisingly not helpful.

What is a proper definition of set?

There isn't one.

Set is a primitive notion of mathematics based on axiomatic set theory.

Cantor: "We take a set to be an assemblage of definite, perfectly distinguishable objects of our intuition or our thought into a coherent whole."

This is surprisingly not helpful.

What is a proper definition of set?

There isn't one.

Set is a primitive notion of mathematics based on axiomatic set theory.

... unless you're into type theory.

In practice we gloss over the problems by using a "naive" set theory, assuming that:

A **set** is a well-defined collection of distinct objects. A set is itself an object.

Naive because well-defined is not very well-defined.

Objects within the set are called **elements** of the set.

- 1. A set may consist of any distinguishable objects
- 2. A set is unambiguously determined by the collection of objects that comprise it.
- 3. Any property defines the set of objects having that property.

When there is no ambiguity a small abuse of notation is ok: $\{x\} = x$.

The elements of a set can be just about anything: numbers, points in space, or even other sets. The conventional way to write down a set is to list the elements inside curly-braces.

$\{$  , ,  $\}$, $\{1, 2, 3, 4\}$, $\{\{a, 2\}, \{c, 5\}\}$ etc...

Order within $\{\}$ does not matter.

There are two ways to write down a set.
1. The simplest one is to **enumerate all elements**.
$\{\circledcirc, \square, \triangle\}$, $\{1, 2, 3, 4\}$, $\{\{a, 2\}, \{c, 5\}\}$ etc...

Works well for finite sets.

Works ok if logic is clear (can abbreviate):
$\{1, 2, 3...999, 1000\}$ etc...

Doesn't work for infinite sets.

2. **Set-builder notation**: a rule that describes how to construct a set (a "class"). The rule is called a predicate.

$$S = \{\{x, y\} : x + y \leq 1, x \in \mathbb{R}, y \in \mathbb{R}\}$$

$$S = \{\{x, y\} | x + y \leq 1, x \in \mathbb{R}, y \in \mathbb{R}\}$$

The set of all letters *I* in the word *team*.

The set of all sets.
This notion is contradictory

Rusell-Zermelo paradox

NST is inconsistent

Proof (from Zorich).
Suppose that for a set M, $P(M)$ means M is not an element of itself.
Consider the class $K = \{M|P(M)\}$ of sets having property P
If K is a set either $P(K)$ or $\neg P(K)$.
If $P(K)$, then $K \in K$, then $\neg P(K)$.
If $\neg P(K)$, then $K \in K$, then K is not $\{M|P(M)\}$.
□

Axiomatic set theory ZFC distinguishes classes and sets, and thus does not claim that $P(K)$ exists. This solves the paradox. We will just ignore the paradox.

Some special sets have assigned symbols, usually written in

$$\mathbb{BLACKBOARD\ BOLD}.$$

$\emptyset = \{\}$ the empty set
$\mathbb{N} = \{0, 1, 2, 3...\}$ or $\mathbb{N} = \mathbb{Z}^+ = \{1, 2, 3...\}$
$\mathbb{Z} = \{...-3, -2, -1, 1, 2, 3...\}$ integers
$\mathbb{Q} = \{\frac{1}{2}, -\frac{5}{3}, 16...\}$ rational numbers
$\mathbb{R} = \{\pi, e, -9, \sqrt{2}\}$ real numbers
$\mathbb{R}_+ = \{\pi, e, 9, \sqrt{2}\}$ positive real numbers
$\mathbb{R}_- = \{-\pi, -e, -9, -\sqrt{2}\}$ negative real numbers
$\mathbb{C} = \{i, \frac{19}{2}, -2i\}$ complex numbers
$\mathbb{R}^2 = \{\{1, 5\}, \{i, -1\}, \{5, \pi\}\}$ tuples of two real numbers

Let $S = \{a, d, o\}$. Usually sets are UPPERCASE, elements are lowercase.
$a \in S$: a is an element of set S
$b \notin S$: b is not an element of set S
$A \subseteq B$: A is a subset of set B. Every element of A is also an element of B, e.g. $\mathbb{N} \subseteq \mathbb{Z}$.
$A \subset B$: A is a strict/proper subset of set B, $A \subseteq B, A \neq B$.
$\mathbb{C} \not\subseteq \mathbb{R}$.
$A \subset B$: A is a strict subset of B, or $A \subseteq B$ and $A \neq B$.
Practice: write the definitions with logic notation.

union $A \cup B$: $x \in A \cup B$ iff $x \in A$ or $x \in B$
intersection $A \cap B$: iff $x \in A$ and $x \in B$.
set difference $A - B$ or better $A \setminus B$: $x \in A \setminus B$ iff $x \in A$ and $x \notin B$.

Usually we have a universe, a domain where we operate.
complement $\bar{A} = D \subseteq A$: complement of A, e.g. if $D = \mathbb{Z}$ then $\bar{\mathbb{N}} = \mathbb{Z}^-$.
If we have these, we can rewrite any $\subseteq$:
$A \subseteq B$ is equivalent to $A \cap \bar{B} = \emptyset$.

de Morgan rules

$A \bar{\cup} B = A \cap B$
$A \bar{\cap} B = A \cup B$

Do these look familiar? Practice: prove the rules.
Venn diagrams help (see attached file)

(x, y) - ordered pair (not a set!)

Cartesian product of sets:

$$X \times Y = \{(x, y) | (x \in X) \wedge (y \in Y)\}$$

$X \times Y \neq Y \times X$ in general. Only if $X = Y$ and then we write X^2 (hence the notation above)

The set of all the subsets of a set A is called a power set. We denote it 2^A. $B \in 2^A$ if $B \subseteq A$.

Why notation 2^A?

$X = Y$ means $z \in X$ iff $z \in Y$ for all z

Distributive law:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

Proof!

$$z \in A \cap (B \cup C) \iff$$

$$(z \in A) \text{ AND } (z \in B \cup C) \iff \qquad \text{(def of } \cap\text{)}$$

$$(z \in A) \text{ AND } (z \in B \text{ OR } z \in C) \iff \qquad \text{(def of } \cup\text{)}$$

$$(z \in A \text{ AND } z \in B) \text{ OR } (z \in A \text{ AND } z \in C) \iff$$

(AND is distributive)

$$(z \in A \text{ AND } z \in B) \text{ OR } (z \in A \text{ AND } z \in C) \iff \qquad \text{(def of } \cap\text{)}$$

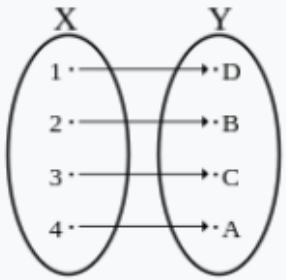
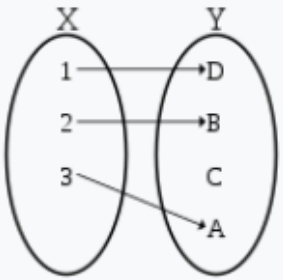
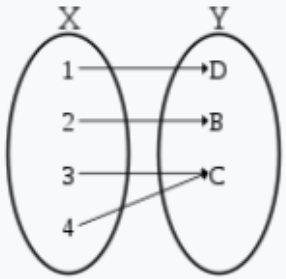
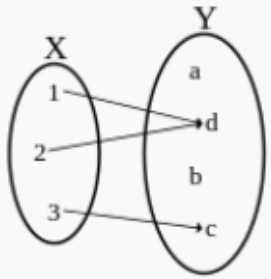
$$(z \in A \cap B) \text{ OR } (z \in A \cap C) \iff \qquad \text{(def of } \cap\text{)}$$

$$(z \in A \cap B) \cup (z \in A \cap C) \iff \qquad \text{(def of } \cup\text{)}$$

Other data types: orders, relations, graphs which are also sets...

A **function** associates to each element of a set X **(domain)** a unique element of a set Y **(codomain)**.

Composition of $f : X \to Y$ and $g : Y \to Z$:
$g \circ f : X \to Z$
$(g \circ f)(x) = g(f(x))$

	surjective	non-surjective
injective	 bijective	 injective-only
non-injective	 surjective-only	

$$f(x) = x^2$$

$$f(x) = Ax$$

$$f(x) = 2x + 3$$

$$D(f) = \textit{derivative of function } f$$

$$sgn(x) := \begin{cases} -1 \text{ if } x < 0, \\ 0 \text{ if } x = 0, \\ 1 \text{ if } x > 0 \end{cases}$$

$$f(x) = \textit{rotation of } x \textit{ by } 10^\circ \textit{ and scaling it by } 1.5$$

$$f(x) = (1 \textit{ iff } x = 1, 0 \textit{ otherwise})$$

$$f(x) = \{3 \textit{ top students}\}, x \in \textit{GMU Classes}$$

$$f(x) = \sum_i x_i,$$

e.g. $f(x) = \sum_{i=1}^{3} x_i$, $x \in \mathbb{R}^3$.

A function that takes a $x \in \mathbb{R}^3$ and returns the closest primary color.

A function that takes a $x \in \mathbb{R}^n$ and returns the number of primes in a set.

Economics:

Choice function

Matching

Supply/Demand

Function returning Pareto outcomes

Expected value of a random variable

Variance

Integral

What is **not** a function?

Definition

A **binary relation** (or a correspondence) between sets A and B is a subset of $A \times B$.

A function is a binary relation with two properties:
1) functionality: for all $x \in X, y, z \in Y$, if xRy, xRz then $y = z$.
2) left-totality: for all $x \in X$, exists $y \in Y$, such that xRy.
Without left-totality it is called a partial function.

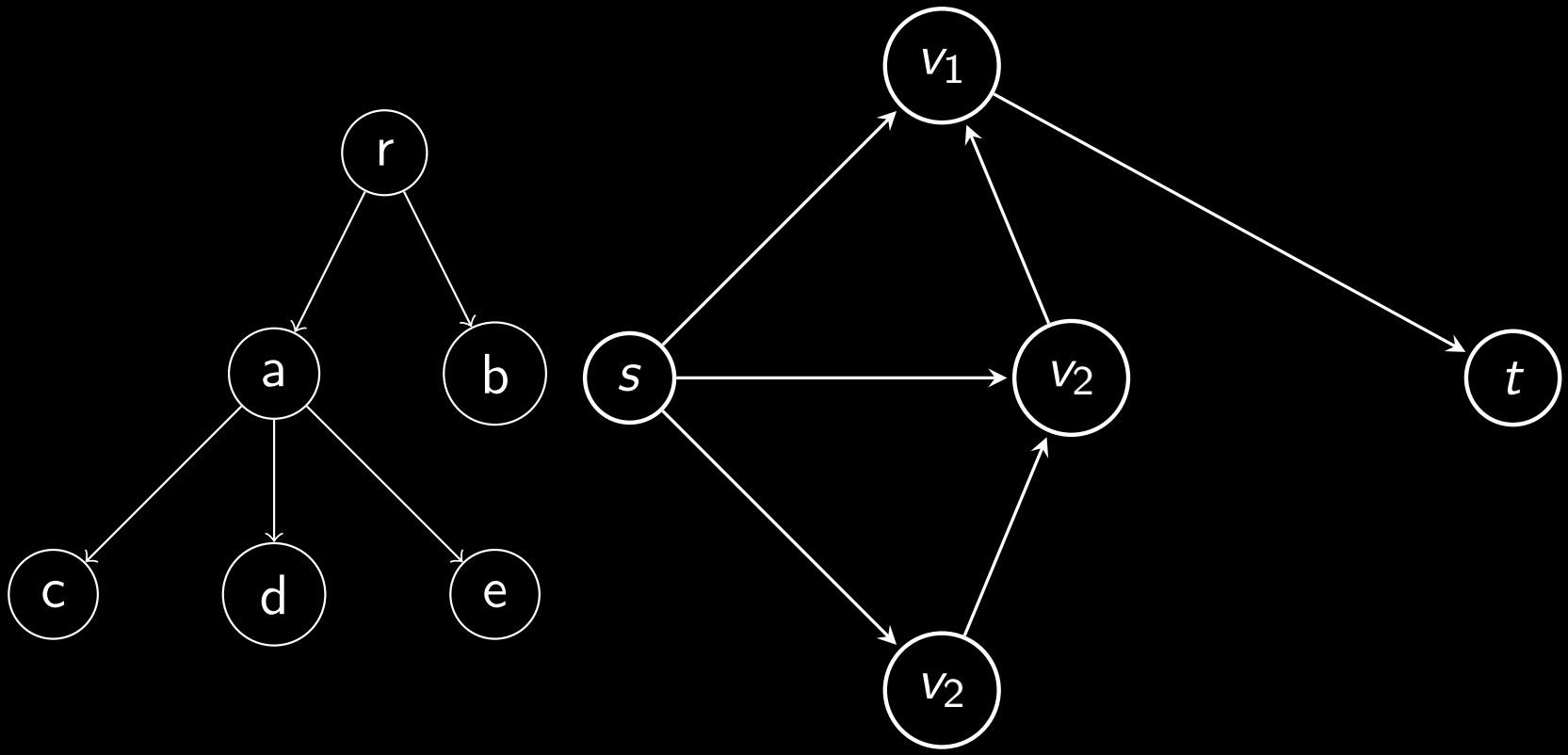
With functions we usually use formulas to define them. With relations, we use sets: for some relation R we say aRb to mean $(a, b) \in R$. The whole table, the subset of $A \times B$ is called a **graph** of a function.

Definition

The inverse, R^{-1} of a relation $R : A \to B$ is the relation from B to A defined by the rule $bR^{-1}a$ iff aRb.

Definition

A graph is a structure amounting to a set of objects in which some pairs of the objects are in some sense "related"



Orders are another type of binary relation (along with functions). **order theory** and **measurement theory** describe statements such as "this is less than that" or "this precedes that".

Economists use orders to describe "ordinal" things like preferences:

$100\$ \succeq 50\$$
$TV \succeq books$
$apples \succeq oranges$

a binary relation $\preceq$ is a total order on a set X if
$\forall a, b, c \in X$
Either $a \preceq b$, or $b \preceq a$. $a \preceq b$, or $b \preceq c$ then $a \preceq c$ (transitivity)
$a \preceq b$ and $b \preceq a$ then $a = b$ (antisimmetry)
A total order on a set with k elements induces a bijection with the first k natural numbers.

Why care about orders?
Measurement - assigning numbers or other symbols to things in such a way that relationships of the numbers or symbols reflect relationships of the attributes of the things.

Measurement theory helps us to avoid making meaningless statements.
Weatherman on the local TV station: it was twice as warm today as yesterday because it was 40 F today but only 20 F yesterday.
Fahrenheit is arbitrary. The relationship 'twice-as' applies only to the numbers, not the attribute being measured (temperature).
– Warren S. Sarle

We have enough math to build three constructs from math econ:
choice function, $c : 2^X \to X$
utility function, $u : X \to \mathbb{R}$
preference relation. $\preceq \subseteq X \times X$
We can leave it at that.

Measuring sets

If A is a finite set, the cardinality $|A|$ of A is the number of elements in A.

Lemma

For finite sets A,B:

1. *If A surj B* ($A \twoheadrightarrow B$), *then* $|A| \geq |B|$.
2. *If A inj B* ($A \hookrightarrow B$), *then* $|A| \leq |B|$.
3. *If A bij B* ($A \leftrightarrow B$) $|A| = |B|$.

Theorem

For finite sets A,B: 1. $\exists$ *A surj B* $(f : A \twoheadrightarrow B)$ *iff* $|A| \geq |B|$.
2. $\exists$ *A inj B* $(f : A \hookrightarrow B)$ *iff* $|A| \leq |B|$.
3. $\exists$ *A bij B* $(f : A \leftrightarrow B)$ *iff* $|A| = |B|$.

We have the machinery to prove result from before:

Theorem

There are 2^n subsets of an n-element set. That is, $|A| = n$ implies $|2^A| = 2^n$:

We just need a bijection to a set that is easier to count.

(Product Rule). If all P_i are finite sets, then:
$|P1 \times P2 \times ...P_n| = \prod |P_i|$

(Sum Rule). If all P_i are disjoint sets, then:
$|P_1 \cup P_2 \cup ...P_n| = \sum |P_i|$.

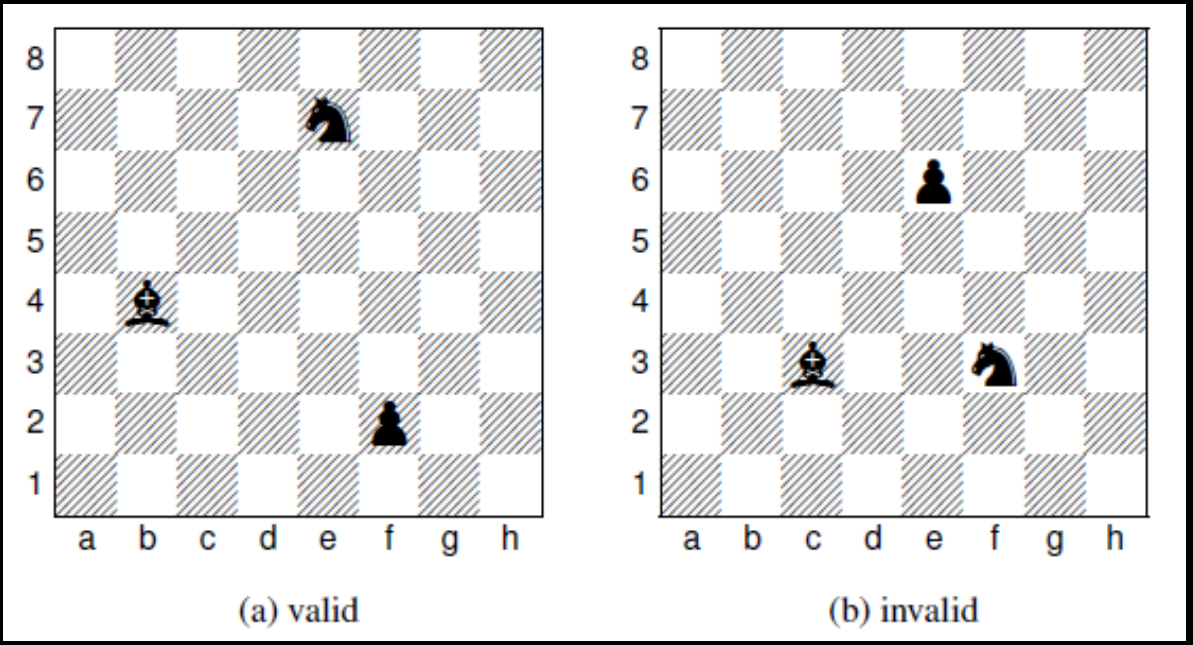
The Bijection Rule: Counting One Thing by Counting Another.

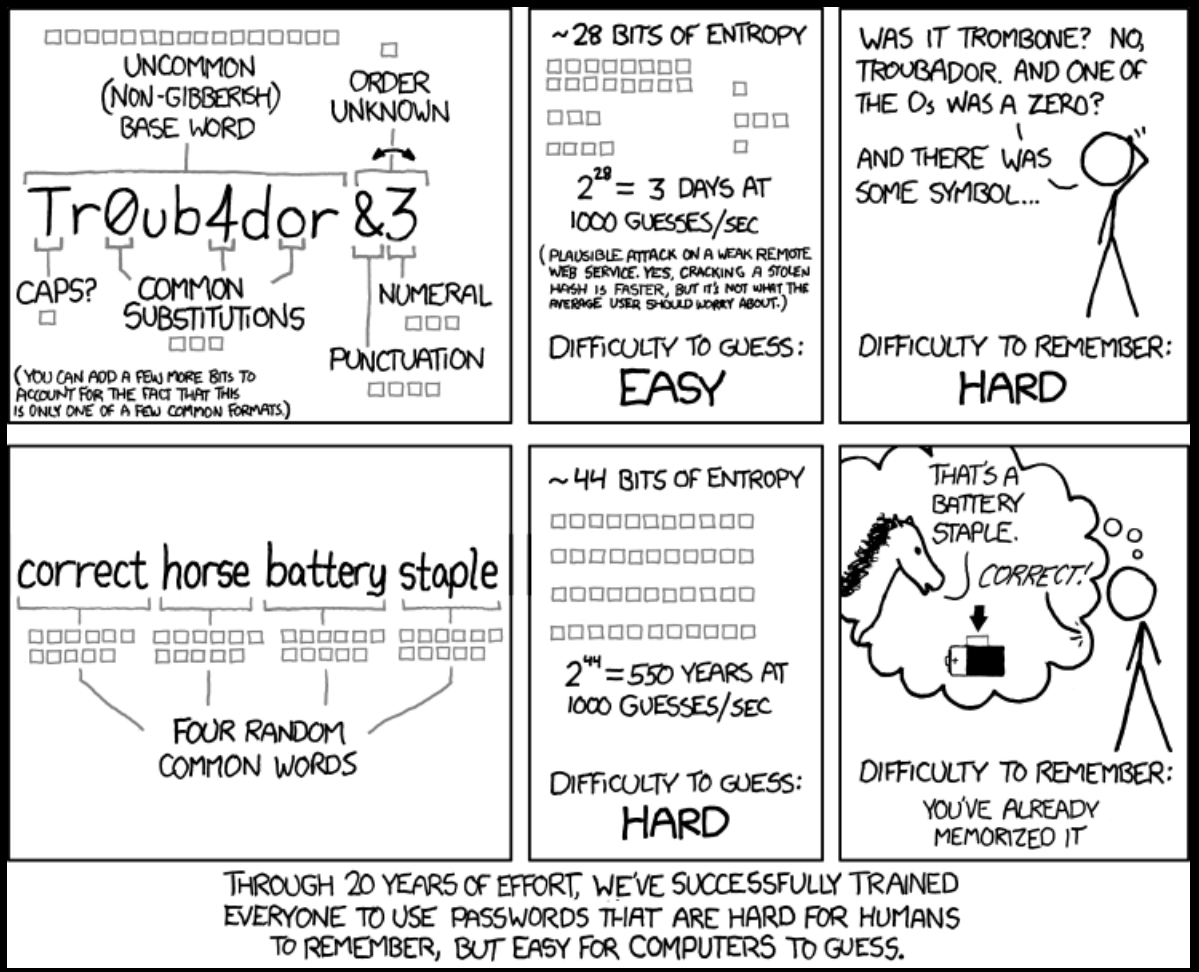
Think in terms of sequences in other numeral systems and images of functions.

12 donuts out of 5 different flavors?

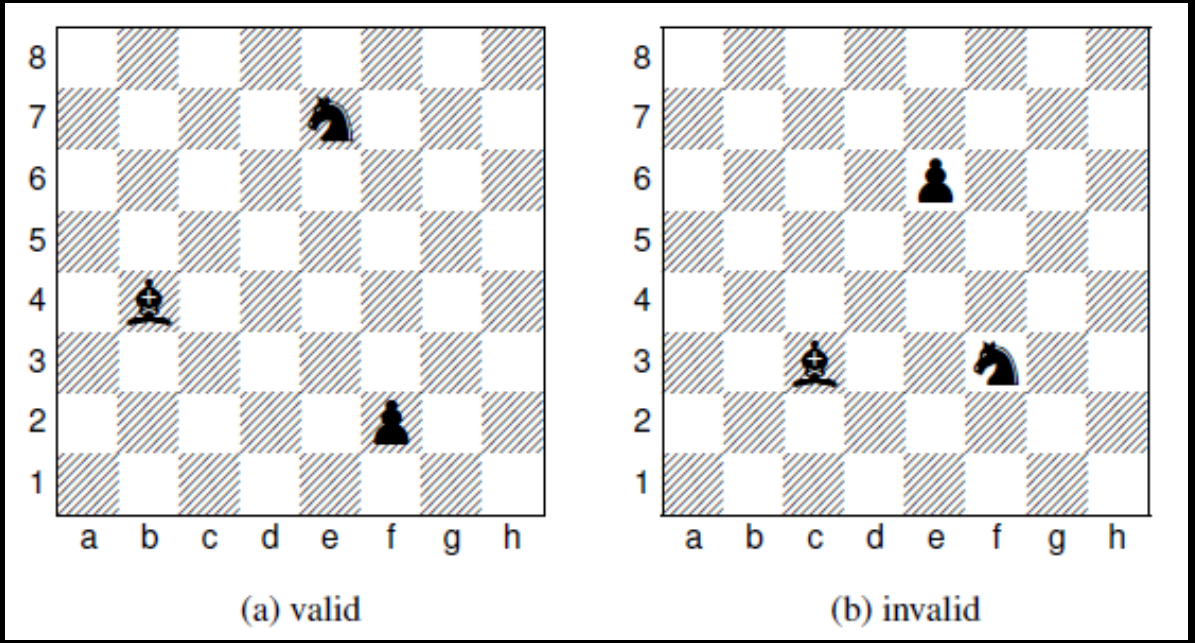
Practice:
k items to distribute between n people. How many possibilities?
3 public goods and 4 private goods?
Multi-period decision problem: How many possible strategies are there?
Number of "strong" passwords: first letter capped, one of four punctuation signs and a number in the end (in any order), 10 digits total.

Base/Radix	Name
2	Binary
8	Octal
10	Decimal
12	Duodecimal (dozenal)
16	Hexadecimal
20	Vigesimal
60	Sexagesimal


8
7
6
5
4
3
2
1
a b c d e f g h
(a) valid
8
7
6
5
4
3
2
1
a b c d e f g h
(b) invalid



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.



A) Knight, bishop and pawn

$$8^2 \times 7^2 \times 6^2$$

B) Three bishops

$$\frac{8^2 \times 7^2 \times 6^2}{6}$$

Define a mapping f : *chessboards* $\to S \subseteq \mathbb{N}^6$, where S is the subset of sequences of six natural numbers.

Let $f(x) = b_1, b_2, k_1, k_2, p_1, p_2$, where b_1, b_2 are row and column of bishop, etc. If $k_1 < b_1$, k_1 is row of knight, otherwise $k_1 =$ row of knight - 1. Similarly for the column, and for the pawn.

For A) this is a bijective mapping. Every chessboard can be uniquely defined by six numbers $(1..8), (1..8), (1..7), (1..7), (1..6), (1..6)$. The result follows by bijection rule.

For B) Assume the same mapping f. Note that f is a surjective function. Chessboards:
$(1, 2, 3), (1, 3, 2), (2, 3, 1), (2, 1, 3), (3, 2, 1), (3, 1, 2)$ are equivalent in problem B, so f maps each element to 6. Therefore the cardinality of the set is that of the problem A divided by 6. (We implicitly combine every set of permutations into one and define a bijection from it to use the bijection rule)

Why not stick with finite sets of some large, but bounded, size?

Math for CS answer

You may not have noticed, but up to now you've already accepted the routine use of the integers, the rationals and irrationals, and sequences of them. These are all infinite sets.

Simple answer - it will come up in your classes.
Longer answer - $[0, 1] \cap \mathbb{R}$ is bounded, but infinite. E.g. share of work and rest.

Definition

A set C is countably infinite ($\aleph_0$) iff N bij C. A set is countable iff it is finite or countably infinite. A set is uncountable iff it is not countable.

Countable sets: $\mathbb{N}, \mathbb{Z}, \mathbb{Z}^+, \mathbb{N} \times \mathbb{N}$... (try constructing a bij).
$2^{\mathbb{N}}, \mathbb{R}$ are uncountable.

Power sets have higher cardinality than the set itself
$2^{\aleph_0} > \aleph_0$

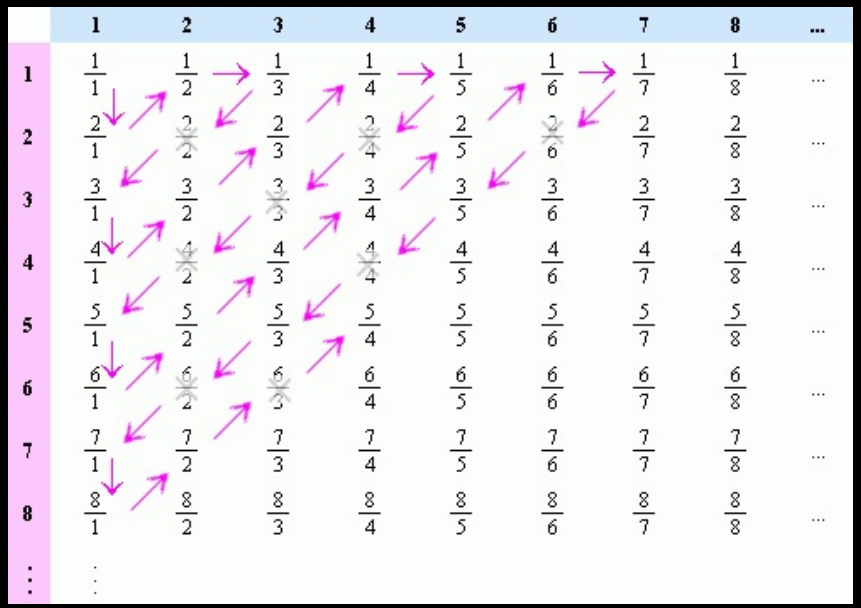
This is more than enough for classes, where countable/uncountable is enough of a distinction. If you like thinking about infinitites, read the textbook.

Practice: Show that the set of rational numbers $\mathbb{Q}$ is countable.

Every $q = \frac{a}{b} \in \mathbb{Q}$ is a tuple of $a, b \in Z \times Z$.

$$\Phi(q) = \begin{cases} 0 & q = 0 \\ 1 & q = 1 \\ -1 & q = -1 \\ 2^m(2n+1) & q = \frac{m}{n} \text{ simplest form} \\ -2^m(2n+1) & q = -\frac{m}{n} \text{ simplest form} \end{cases}$$

Alternatively reorder them so that

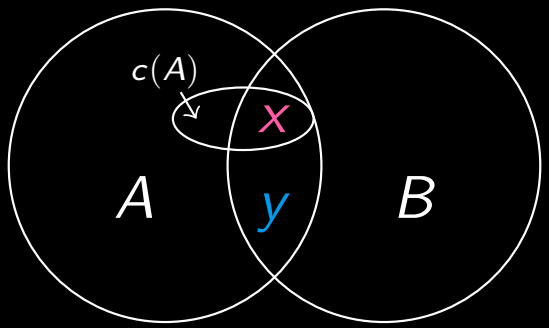


A reasonable question: why should economists care?

Math Econ II example: **choice coherence**

Theorem

Let $x, y \in X$ $A, B \in \mathcal{A}$ and $x, y \in A \cap B$
The following two definitions are equivalent:
$x \in c(A)$ *and* $y \notin c(A) \implies y \notin c(B)$.
$x \in c(A)$ *and* $y \in c(B) \implies y \in c(A)$ *and* $x \in c(B)$.



Math for CS (chapters 1 and 5)
https://courses.csail.mit.edu/6.042/spring17/mcs.pdf

Part 3: Proofs

- Theorem - main result
- Proposition - smaller result
- Lemma - intermediate step in the proof, to chop it to pieces.
  - But sometimes they escape, as Zorn's lemma did. - Gerald Edgar @ stackoverflow

"If you are proud of a result, call it a Theorem. If not, it is a Proposition."

Definition

A **proposition** is a statement (communication) that is either true or false.

Axiomatic method:

A **proof** is a sequence of logical deductions from axioms and previously proved statements that concludes with the proposition in question.

Zermelo–Fraenkel set theory (ZFc)

Infinity, Union, Power set, Extensionality, Restricted comprehension, Pairing, Regularity, Schema of replacement, Well-ordering principle + choice (independent dark horse anti-hero that sometimes joins)

–two cubes @ tumblr

The axioms are usually extremely basic, e.g.

Power set, just says that for any set x there also is 2^x, defined the way we did before.

Definition (Well ordering principle)

Every nonempty set of nonnegative integers has a smallest element.

or

Definition

The set of positive integers does not contain any infinite strictly decreasing sequences.

Prove $P \implies Q$

Method 1: Direct proof

1. Write "Assume P."
2. Show that Q.

Theorem

If $0 \leq x \leq 2$ *then* $-x^3 + 4x + 1 > 0$

- Inspect, notice that $x = 0$ works.

Theorem

If $0 \leq x \leq 2$ *then* $-x^3 + 4x + 1 > 0$

- Inspect, notice that $x = 0$ works.
- $4x$ and $-x^3$ are competing for power and are growing at different speed. Notice that for $4x$ the derivative is constant, and for $-x^3$ it is a polynomial of power 2. So ultimately one will overtake the other at exactly one point. Note that this point is 2: $-x^3 > 4x$ for $x > 2$. If this is true then the "theorem" follows.
  We can factor that part: $-x^3 + 4x = x(2 - x)(2 + x)$, which is nonnegative for $x \in [0, 2]$.

Theorem

If $0 \leq x \leq 2$ *then* $-x^3 + 4x + 1 > 0$

Proof.

Assume $0 \leq x \leq 2$. Then $x, 2 - x$ and $2 + x$ are all nonnegative. Therefore, the product of these terms is also nonnegative. Adding 1 to this product gives a positive number, so:

$$x(2 - x)(2 + x) + 1 > 0$$

Multiplying out on the left side proves that

$$-x^3 + 4x + 1 > 0$$

as claimed. □

Method 2: Prove the *contrapositive* $P \implies Q$ is equivalent to $\neg Q \implies \neg P$

1. Write "We prove the contrapositive", state the contrapositive.
2. Prove as in Method 1

Theorem

If r is irrational, then $\sqrt{(r)}$ is also irrational.

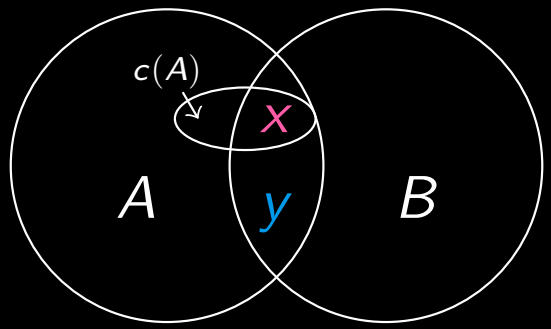
Proof.

We prove the contrapositive: if $\sqrt{r}$ is rational, then r is rational.
Assume $\sqrt{r}$ is rational. Then there are integers m and n:
$\sqrt{r} = \frac{m}{n}$, $r = \frac{m^2}{n^2}$
Since m^2 and n^2 are integers, r as rational. □

Economics example: **choice coherence**

Theorem

Let $x, y \in X$ $A, B \in \mathcal{A}$ and $x, y \in A \cap B$
The following two definitions are equivalent:
$x \in c(A)$ *and* $y \notin c(A) \implies y \notin c(B)$.
$x \in c(A)$ *and* $y \in c(B) \implies y \in c(A)$ *and* $x \in c(B)$.



Option a) Contrapositive

$x \notin c(A)$ or $y \in c(A) \impliedby y \in c(B)$.

Replace A with B and x with y:

$y \notin c(B)$ or $x \in c(B) \impliedby x \in c(A)$.

Combine the two, and we get the claim.

Option b) use the implication formula $(p \implies q) = (\neg p \vee q))$

Proof of ($\Longleftarrow$)

Assume $x \in c(A)$ and $y \in c(B) \implies y \in c(A)$ and $x \in c(B)$.
Contrapositive and negation with DeMorgan laws:
$\neg x \in c(A)$ or $\neg y \in c(B) \Longleftarrow \neg y \in c(A)$ or $\neg x \in c(B)$.
Or in other words
$y \notin c(A)$ or $x \notin c(B) \implies x \notin c(A)$ or $y \notin c(B)$.
So since either one implies the right part, we can write this as two implications:
$y \notin c(A) \implies x \notin c(A)$ or $y \notin c(B)$.
$x \notin c(B) \implies x \notin c(A)$ or $y \notin c(B)$.
So in the case when $x \in c(A)$, we would have only $y \notin c(B)$ in the right part (this is akin to informally adding $x \in c(A)$ on both sides with an and. So:
$y \notin c(A)$ and $x \in c(A) \implies y \notin c(B)$ $\square$.

In fact this is almost a chain of $\Longleftrightarrow$, except for the middle part, so the converse is almost the same.

Proving $\iff$:

Method 1: Prove each statement implies the other, i.e. sufficiency and necessity.

S	N	$S \implies N$	$N \implies S$	$S \iff N$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

In terms of notation, either write "Suffiency" and "Necessity" for the two parts of the proof or just use ($\Longrightarrow$) ($\Longleftarrow$). Convention is to start the condition with something of importance and then follow it by condition, e.g.

Theorem

Two triangles have the same side lengths (P) if and only if two side lengths and the angle between those sides are the same (Q).

Proof.

Two parts:

($\Longrightarrow$) That is $P \implies Q$ so Q is necessary condition for P

($\Longleftarrow$) That is $Q \implies P$ so Q is sufficient condition for P $\square$

Method 2: Construct a Chain of Iffs

Prove P is equivalent to a second statement which is equivalent to a third statement and so forth until you reach Q.

Let's agree that given any two people, either they have met or not. If every pair of people in a group has met, we'll call the group a club. If every pair of people in a group has not met, we'll call it a group of strangers.

Theorem

Every collection of 6 people includes a club of 3 people or a group of 3 strangers.

Proof. The proof is by case analysis.
Let x denote one of the six people. There are two cases:
1. Among 5 other people besides x, at least 3 have met x. 2. Among the 5 other people, at least 3 have not met x.

Theorem

Every collection of 6 people includes a club of 3 people or a group of 3 strangers.

Proof. The proof is by case analysis.
Let x denote one of the six people. There are two cases:
1. Among 5 other people besides x, at least 3 have met x. 2. Among the 5 other people, at least 3 have not met x.
(Note that these cases are complements and cover all possibilities)
Case 1:
Case 1.1: No pair among those people met each other. Then these people are a group of at least 3 strangers. The theorem holds in this subcase.
Case 1.2: Some pair among those people have met each other. Then that pair, together with x, form a club of 3 people. So the theorem holds in this subcase.

Case 2: Suppose that at least 3 people did not meet x. This case also splits into two subcases:
Case 2.1: Every pair among those people met each other. Then these people are a club of at least 3 people. So the theorem holds in this subcase.
Case 2.2: Some pair among those people have not met each other. Then that pair, together with x, form a group of at least 3 strangers. So the theorem holds in this subcase.

1. "Suppose P is false."
2. Deduce something known to be false (a logical contradiction).
3. Write, "This is a contradiction. Therefore, P must be true."

Proving that $\sqrt{2}$ is irrantional can be done by contradiction:

Theorem

$\sqrt{2}$ is irrational.

Proof.

We proceed by contradiction. Suppose $\sqrt{2}$ is rational, $\sqrt{2} = \frac{n}{d}$, simplest form.
Square: $2 = \frac{n^2}{d^2}$, so $2d^2 = n^2$. n is a multiple of 2
Then n^2 is even, but then n is also even. But then n^2 is divisible by 4. Then q^2 and q are even. So there is a common factor of 2, which is a contradiction. □

Theorem

$\sqrt{2}$ is irrational.

Proof.

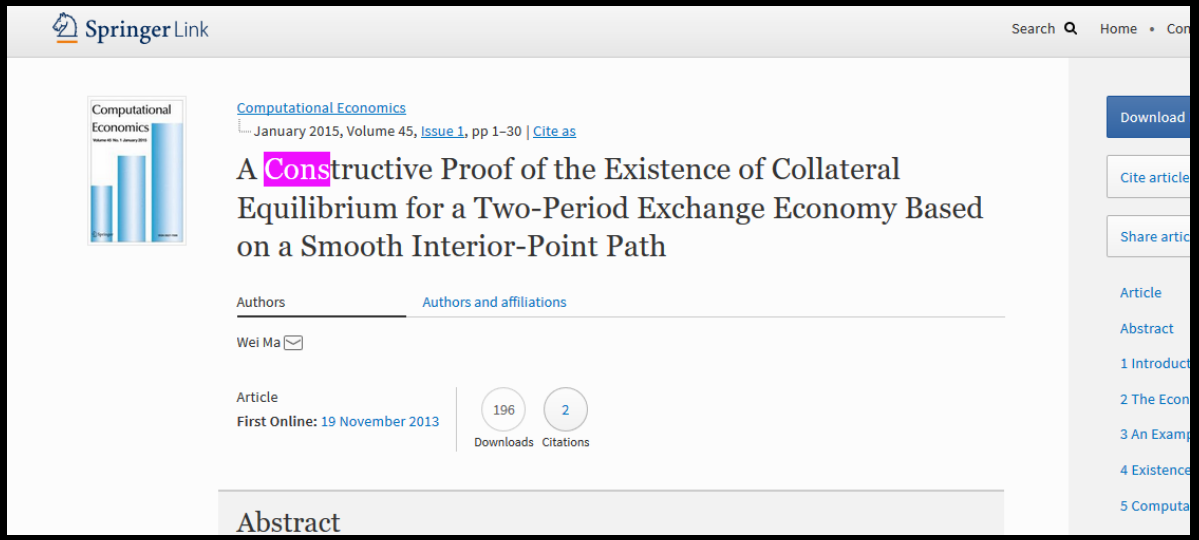
We proceed by contradiction. Suppose $\sqrt{2}$ is rational, $\sqrt{2} = \frac{n}{d}$, not necessarily simplest form.
Square: $2 = \frac{n^2}{d^2}$, so $2d^2 = n^2$. n is a multiple of 2
Then n^2 is even, but then n is also even. But then n^2 is divisible by 4. Then q^2 and q are even. So there is a common factor of 2, which means for every rational number there is another rational number with smaller n and d ad infinitum. But this violates the well-ordering principle. □

A very classic example:
Power of an Irrational Number to an Irrational Exponent May Be Rational

Proof.

$\sqrt{2}^{\sqrt{2}}$ is either rational or irrational. If it is rational, our statement is proved. If it is irrational, $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$ proves our statement. □

This uses law of excluded middle and is not constructive, there is no example built.
$a = \sqrt{2}$, $b = log_2 9$, $a^b = 3$ would be a constructive proof.



In econ people also usually hope to see the constructed object. An existential proof would indicate that people will reach an equilbrium, but, ideally, we would like to see what this equilibrium is like (e.g. in closed form in terms of parameters).

Definition

The Induction Principle. Let P be a predicate on nonnegative integers. If
$P(0)$ is true (base), and
$P(n) \implies P(n+1)$ for all nonnegative integers n (step)
$P(m)$ is true for all nonnegative integers m.

Examples are rudely stolen from Math for CS textbook and reframed for Mason.

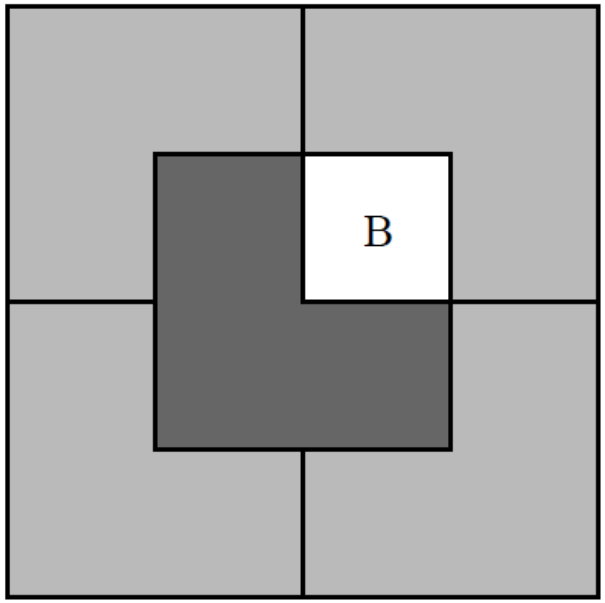
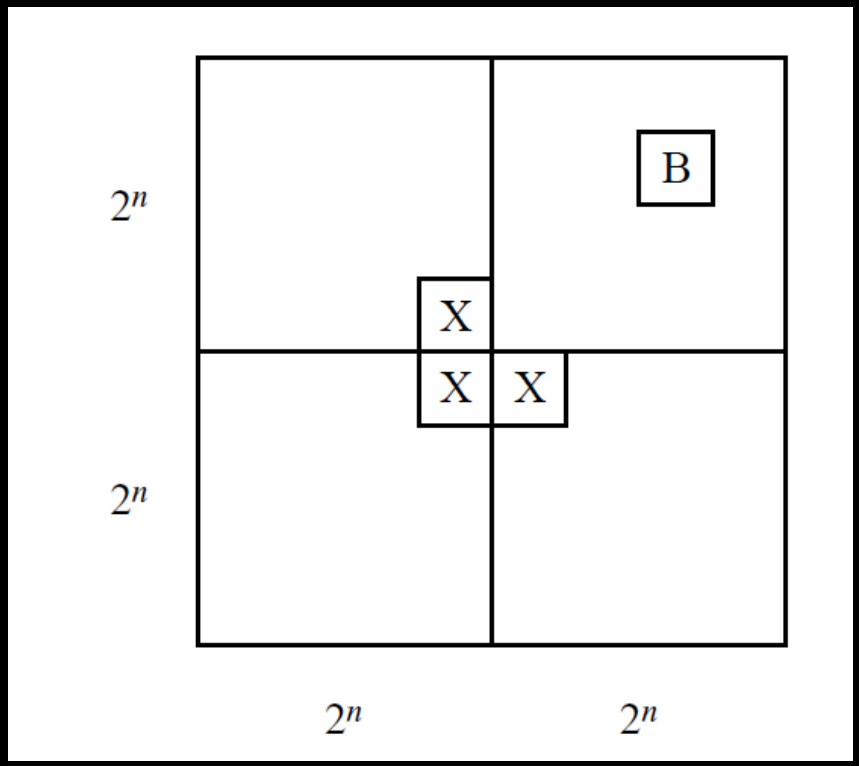
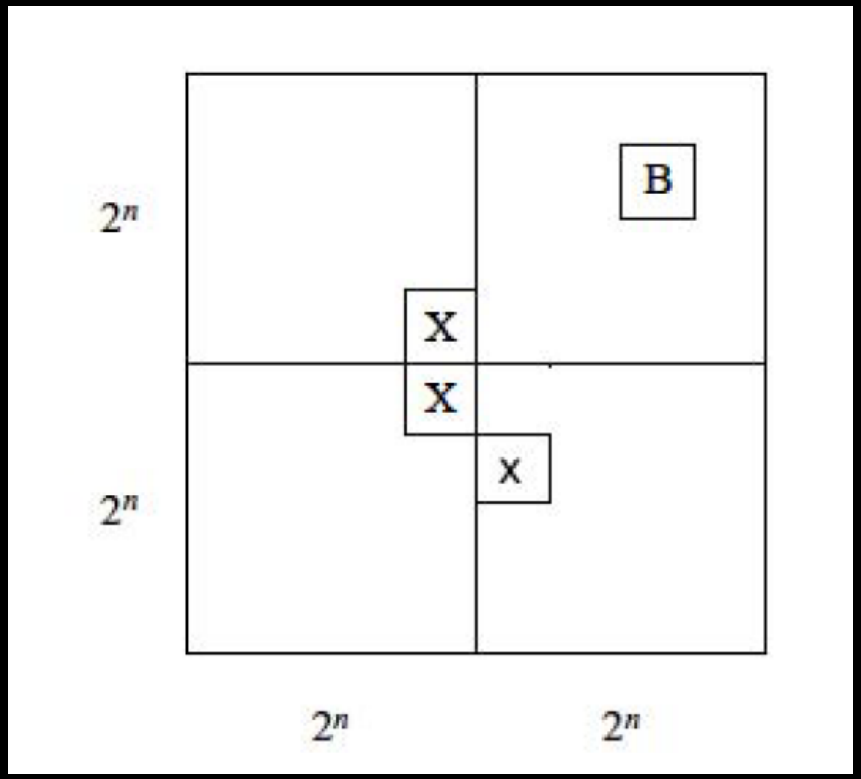


Figure 5.3 A tiling using L-shaped tiles for $n = 2$ with Bill in a center square.


B
X
X
X
2^n
2^n
2^n
2^n

Quick textbook problem:



Can we use the same claim? Why not?

Definition

The Strong Induction Principle. Let P be a predicate on nonnegative integers. If
$P(0)$ is true (base), and
$P(0), P(1), P(2)...P(n) \implies P(n+1)$ for all nonnegative integers n (step)
$P(m)$ is true for all nonnegative integers m.

Coins worth 3Mm and 5Mm. Prove that anyone can make change for any number ≥ 8.

Proof.

Assume $P(k)$ holds for all $k \leq n$ and prove $P(n+1)$ holds.
Case $(n+1=1)$: We have to make $(n+1)+8 = 9Mm$. This can be done with 3 3Mm coins.
Case $(n+1=2)$: We have to make $(n+1)+8 = 10Mm$. Two 5Mm coins
Case $(n+1 \geq 3)$: $0 \leq n-2 \leq n$ so $(n-2)+8$ is covered. By adding 3Mm coin we arrive to $(n+1)+8$. □

Finally, note that strong-induction and ordinary induction are equivalent.

Let's prove induction.
Use well ordering principle:

Proof.

Suppose P is some property of an integer (that is, a **predicate**), such that $P(1) \wedge P(n)$ implies that $P(n+1)$.
Let S be the set of integers k such that $P(k)$ is false.
Suppose S is nonempty and let k be its least element.
Since $P(1)$ is true, $1 \notin S$, so $k \neq 1$, so $k-1$ is a positive integer, and by minimality $k-1 \notin S$.
So $P(k-1) = T$, but then $P(k)$ is true by "step".
So $k \notin S$, contradiction and $S = \emptyset$. So $P(k) \forall k$. □

In fact you can prove the converse, and induction is thus equivalent to well-ordering principle.

Misc conventions:

- Do not overuse set theoretic notation, if the same can be said in English.
- Then again, when you define objects, use precise definitions like set builder notation. There is usually a balance.
- Start the proof by declaring a method: "We prove by induction" "We prove by contrapositive" etc.
- The main goal is to make the proof readable, i.e. don't use proof by intimidation. See the textbook for more conventions.

Can we automate the process?

- Proof-checking is a relatively simple problem.
- Automated proving is a complicated problem.

Metamath: http://us.metamath.org/mpegif/sqr2irr.html
LEAN
Mathematica:
WolframAlpha["use induction to show that $8^n - 3^n$ is divisible by 5 for $n > 0$"]

Problems from the textbook.

1. Counting passwords
2. Chessboard

Questions.

Thank you

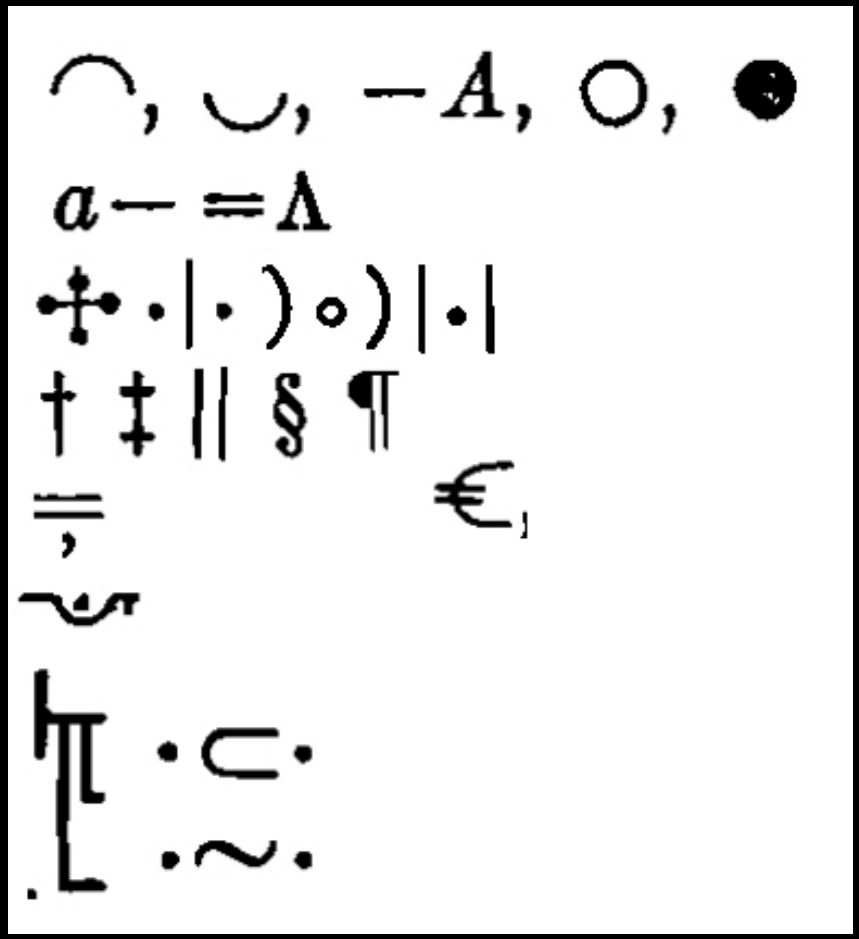


Figure: Some mathematical logic symbols by Boole, De Morgan and other writers