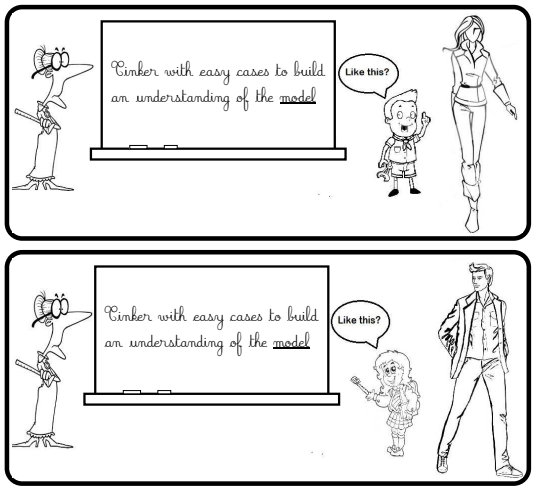
Foundations of Computer Science
Lecture 2

Discrete Objects and Proof

The Cast of Discrete Objects
Some Basic Proofs



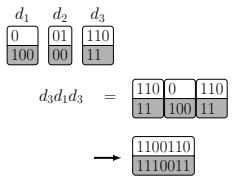
(Niteesh Thangaraj, RPI Class of 2020)

Last Time

A taste of discrete math and computing (ebola, speed dating, friendship networks)

$100
Distinct subsets with the same sum.

$1,000
Domino Program



Goal: Want same top and bottom.

Domino program:
Input: dominos
Output: sequence that works
or
say it can't be done

$10
Create the best 'math'-cartoon.

Create a cartoon to illustrate/make fun of some discrete math you learned in this class.

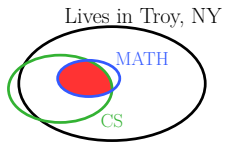
If you submit one, I can use it in the future

Today: Discrete Objects and Proof

1. Discrete Objects
   - Sets
   - Sequences
   - Graphs
2. Proof
   - In 4 rounds of the speed-dating app, no one meets more than 12 people.
   - x^2 is even "is the same as" x is even
   - Among *any* 6 people is a 3-clique or 3-war.
   - **Axioms.** The Well-Ordering Principle.
   - $\sqrt{2}$ is not rational.

Sets

1. Collection of objects, order does not matter: $F = \{f, o, x\}$; $V = \{a, e, i, o, u\}$.
   $F \cap V = \{o\}$ $\quad F \cup V = \{a, e, f, i, o, u, x\}$ $\quad \overline{F} = ?$
2. natural numbers $\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$ What is "…?"
   integers $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \ldots\}$
3. $E = \{2, 4, 6, 8, 10, 12, \ldots\}$ $\quad E' = \{2, 4, 6, 8, 10, 13, \ldots\}$ What is "…?"
4. $E = \{n \mid n = 2k;\ k \in \mathbb{N}\}$ ← no "…" **Pop Quiz:** Define $O = \{\text{odd numbers}\}$.
5. Rational numbers $\mathbb{Q} = \left\{r \,\middle|\, r = \frac{a}{b};\ a \in \mathbb{Z},\ b \in \mathbb{N}\right\}$
6. Subset $A \subseteq B$ (every element of A is in B). $\varnothing \subseteq A$ for any A.
   Power set $\mathcal{P}(A) = \{\text{all subsets of } A\}$ **Pop Quiz:** $A = \{a, b\}$. What is $\mathcal{P}(A)$?
7. Set equality, $A = B$ means $A \subseteq B$ and $B \subseteq A$.
8. Set operations: Intersection, $A \cap B$
   Union, $A \cup B$
   Complement, $\overline{A}$



9. Venn Diagrams are a convenient way to represent sets.

Sequences

- List of objects: order and repetition matter.

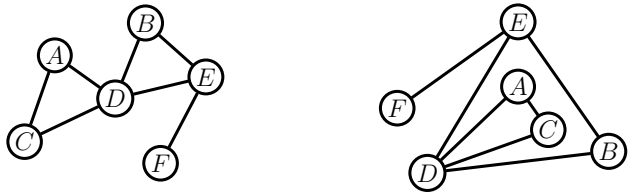
$$tap \neq taap \neq atp$$

- We are mostly concerned with *binary sequences* composed of *bits* (ASCII code).

t	a	p
01110100	01100001	01110000

Graphs

Friendships between Alice, Bob, Charles, David, Edward, Fiona:



$$V = \{A, B, C, D, E, F\}.$$

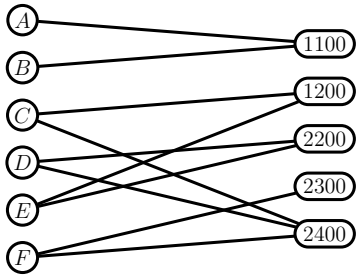
$$E = \{(A, C), (A, D), (C, D), (B, D), (B, E), (D, E), (E, F)\}.$$

What matters is:
who the people are, that is the set V of objects; and,
who is friends with whom, that is the set E of relationships.

The picture with circles and links is a convenient *visualization* of the graph.

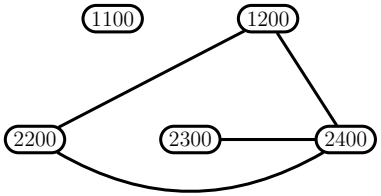
Graphs and Different Types of Relationships

Affiliation graphs



Students and their courses.

Conflict graphs



Courses with students in common conflict. (Why?)

Proof

It is Human to seek verification – proof.

- The sun will rise tomorrow. It has risen every morning in history! (*inductive proof*)

  Do you have any doubts?

- In the speed dating ritual, no-one meets more than 12 people.

  deductive proof:
  In any round a person meets *at most* 3 new people. (Why?)
  There are 4 rounds, *ergo* at most $4 \times 3 = 12$ people can be met.

  Do you have any doubts? That's the beauty of deductive proof.

When is a Number a Square

Tinker!

n	0	±1	±2	±3	±4	±5	±6	±7	±8	±9	±10	±11	$\dots$
n^2	**0**	1	**4**	9	**16**	25	**36**	49	**64**	81	**100**	121	$\dots$

Conjecture.
Even squares come from even numbers and even numbers have even squares.

Proof. (How do I convince you this is true, *without a doubt*?) Let's look at the *cases*

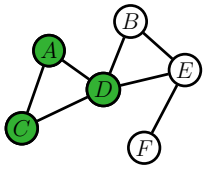
(i) n is even $\rightarrow\ n = 2k\ \rightarrow\ n^2 = 2(2k^2)\ \rightarrow\ n^2$ **is even**.
(ii) n is odd $\rightarrow\ n = 2k+1\ \rightarrow\ n^2 = 2(2k^2+2k)+1\ \rightarrow\ n^2$ **is odd**.

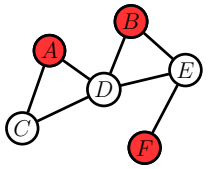
n must be even or odd, and we made no assumptions about n (n is *general*).

Are you convinced? ■

Theorem.
Every even square came from an even number and *every* even number has an even square.

3-war or 3-clique



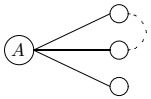


friend clique
war

Theorem.
Any 6-person friend network, has a 3-person friend clique or a 3-person war (or both).

Proof. For a *general* network with 6 people, there are two cases:

(i) A has more friends than enemies.



Two friends are linked → 3-clique.
None are linked → 3-war.

(ii) A has more enemies than friends.

Two friends are enemies → 3-war.
None are enemies → 3-clique. ■

We Can't Prove Everything

- **Axioms:** A self-evident statement that is asserted as true without proof.
- **Conjectures:** A claim that is believed true but is not true until proven so.
- **Theorems:** A proven truth. You can take it to the bank.

Axiom. The Well-Ordering Principle
Any non-empty subset of $\mathbb{N} = \{1, 2, 3, \dots\}$ has a minimum element.
$\{2, 5, 4, 11, 7, 296, 81\}$; or,
$\{6, 19, 24, 18, \dots\}$.

Exercises.

- Construct a subset of $\mathbb{Z}$ (integers) that has no minimum element.
- Construct a positive subset of $\mathbb{Q}$ (rationals) that has no minimum element.

A Gift from Hipassus: $\sqrt{2}$ is Irrational

It may not be so.

In which case $\sqrt{2}$ is rational,

$$\boxed{\sqrt{2}} = \left\{\frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}, \frac{a_4}{b_4}, \dots\right\}$$ ← all possible ways to write $\sqrt{2}$ as a fraction

where $a_1, a_2, \dots$ are all integers and $b_1, b_2, \dots$ are all natural numbers.

Well-ordering principle: there is a minimum b_i, call it b_*.

$\sqrt{2} = a_*/b_*$ and a_* **and** b_* **have no factor in common.** (b_* is the minimum possible)

$$\sqrt{2} = \frac{a_*}{b_*} \quad \rightarrow \quad a_*^2 = 2b_*^2 \quad \rightarrow \quad a_* \text{ is even (why?).}$$

So, $a_* = 2k$ and

$$4k^2 = 2b_*^2 \quad \rightarrow \quad b_*^2 = 2k^2 \quad \rightarrow \quad b_* \text{ is even (why?).}$$

So, a_* **and** b_* **have the factor 2 in common.**

Reductio ad Absurdum

FISHY!

It *must* be so!

A Proof Must Convince

A proof strings together "truths" to *convince* the reader of something *new*.

Our proof that $\sqrt{2}$ is irrational strung together several "truths":

- The well-ordering principle.
- High-school algebra for manipulating equalities.
- Our Theorem on when a square is even.

A proof's goal is always, always, ALWAYS to convince a reader of something.

Making and Proving A Claim

Three Steps for Making and Proving a Claim

Step 1: Precisely state the right thing to prove. Often, creativity and imagination are needed. The claim should be non-trivial, i.e. useful, but also "provable" given the tools you have. Most importantly, the claim should be true (and how do you know that).

Step 2: Prove the claim. Sometimes a simple "genius" idea may be needed. Again, creativity and imagination play a role. Sometimes standard proof techniques can be used; you can become proficient in these techniques through training and practice.

Step 3: Check the proof for correctness. No creativity is needed to look a proof in the eye and determine if it is correct; to determine if you are convinced. Become an expert at this task. Don't allow anyone to claim bogus things and "convince" you with invalid proofs.

Next. How to make precise claims.