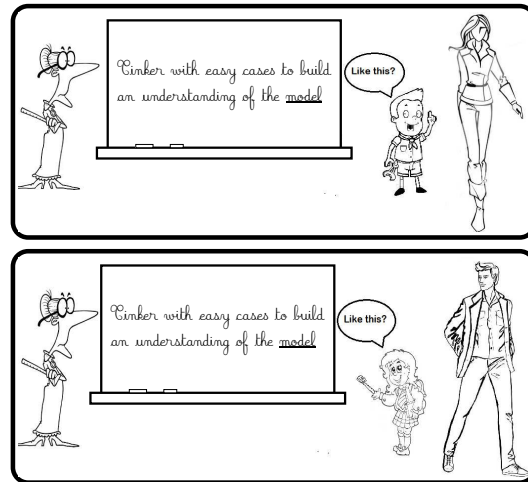


Foundations of Computer Science

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	\$10 Create the best 'math'-cartoon.
<p>571982595957961345054155629 179643904942132605886393</p> <p>3487848284115806672137984 036225211799597044406265</p> <p>476736017145474224377014 9545454545454545454545454</p> <p>18539419597573212586239784 38229118621102318566265796</p> <p>4299778414089787514367977 864178645747496347472950</p> <p>79671389617984549049417196 2902765452022969269167</p> <p>257292779661319022764888 429608977661260713382431896</p> <p>128457419152630693181981 9632764172652474309775483</p> <p>476413835291386389185496 841324241827575412289458</p> <p>14743484182437802296714474 287833244484288182242154</p> <p>427846763661911324828293 489911847797411134873903</p> <p>5611908852668684197738754 4420766779648417179450542</p> <p>22428280984895152838439 7184565949649787844329425</p> <p>7474398414674128675683398 227828135729685774698828</p> <p>62138587349494971748161445 688813271308644576223389</p> <p>842736238496772552648674 3161828678878818881509719224</p> <p>5543645967478383628861178 1917614457892826314778825</p> <p>58549275945941788026747 308481374873781561027784</p> <p>53189117963654131215471 75896465674294145694562221</p> <p>67769174424123146075717625 28797067389719945827984</p> <p>42828981441462284198812 4678454247679797979919817</p> <p>4684847158687462587052344 2821524138293768614076246</p> <p>2636217342827318811879 8754472592825898082678</p> <p>125822627295964978418839 983862675746244576963828</p> <p>4822797276479767054899397 5296712514254243446111278</p> <p>87495222267118296411865 982518291841964382811728</p> <p>1145994179619717968930962 147226144311311478760593</p> <p>38701127586227598242711 2143819142261651651262599</p> <p>9212595107419057168196759 67339765915626622211264</p> <p>351223188187126789197472 21466754447249654938214</p> <p>8858282261512688848976 848172723181878268894746</p> <p>4328594887452255448653 99611728625709527978796</p> <p>24251182759446138171683 59137941452576140743751</p> <p>678484868696125788427653 624217748348484919186096</p> <p>879435172311781289776215 43848491178291287843812902</p> <p>298044845474797015213829 758684284748186318117787</p> <p>6117454479877511848789412 2796215988214612511474323</p> <p>276154480976036844239498 61742991748748741647225</p> <p>698424480976814309787 387941452576140743751</p> <p>8071829138175711730826214 531703137727228488242903</p> <p>943159674143826848883957 6624243155226983896592</p> <p>478448668748858581844469 13140285771329218601662527</p> <p>3024757217714147271137622 2486279672874166838917834</p> <p>9381497429621311712193652 879692978184249249418</p> <p>989311561642424312854454 290271887426347478713813</p> <p>5913228989387768603159862 37914892748766603182899</p> <p>831891545962721460285479 28172771157299987461596</p> <p>220262138187911874612809 328129251467272022716883</p> <p>47748988644145411752214 99241492223678677621974</p> <p>6218496152249624151883878 341433914354124288832878</p>	<p>d_1 d_2 d_3</p> <p>$\begin{bmatrix} 0 & 01 & 110 \\ 100 & 00 & 11 \end{bmatrix}$</p> <p>$d_3 d_1 d_3 = \begin{bmatrix} 110 & 0 & 110 \\ 11 & 100 & 11 \end{bmatrix}$</p> <p>$\rightarrow \begin{bmatrix} 1100110 \\ 1110011 \end{bmatrix}$</p> <p>Goal: Want same top and bottom.</p> <p>Domino program: Input: dominos Output: sequence that works or say it can't be done</p>	<p>Create a cartoon to illustrate/make fun of some discrete math you learned in this class.</p> <p>If you submit one, I can use it in the future</p>

Today: Discrete Objects and Proof

1 Discrete Objects

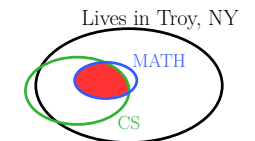
- Sets
- Sequences
- Graphs

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

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



Sequences

- 1 List of objects: order and repetition matter.

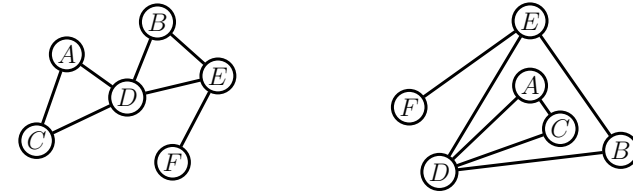
$$tap \neq taap \neq atp$$

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

$$\begin{array}{ccc} t & a & p \\ 01110100 & 01100001 & 01110000 \end{array}$$

Graphs

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



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

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

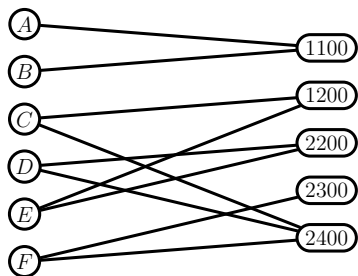
What matters is:

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.

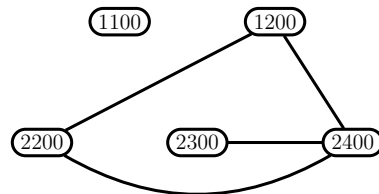
Graphs and Different Types of Relationships

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	...
n^2	0	1	4	9	16	25	36	49	64	81	100	121	...

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.

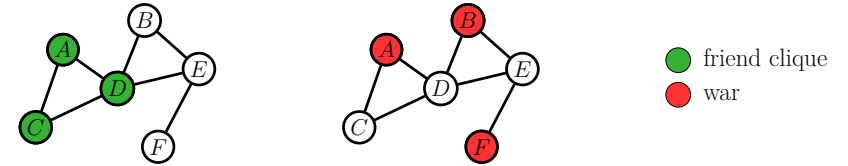
n must be even or odd, and we made no assumptions about n (n is *general*).

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

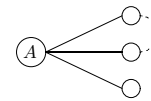


Theorem.

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 \rightarrow 3-clique.

None are linked \rightarrow 3-war.

(ii) A has more enemies than friends.



Two friends are enemies \rightarrow 3-war.

None are enemies \rightarrow 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,

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

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_* , call it b_* .

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

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

So, $a_* = 2k$ and

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

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

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.