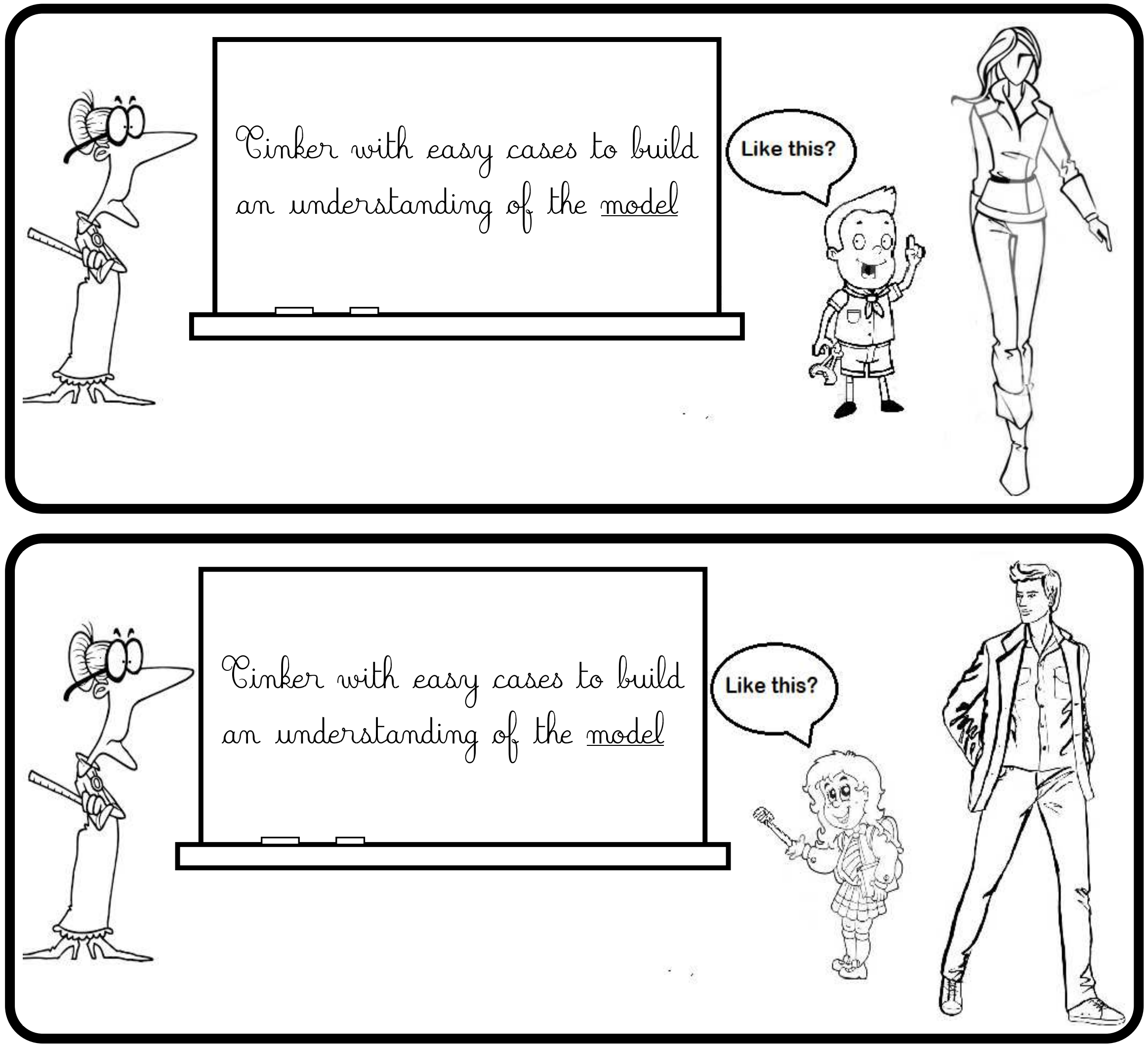
Foundations of Computer Science
Lecture 2

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.

5719825393567961346558155629	1796439694824213266958886393
5487945882843158696672157984	6366252531759955676944496585
4767766531754254874224257763	8545458545636898974365938274
1855924359757732125866239784	3362291186211522318566852576
4289776424589197647513647977	8464473866375474967347772855
7967131961768854889594217186	2892857564355262219965984217
2572967277666133789225764888	4296693937661266715382241936
1294587141921952639693619381	8634764617265724716389775433
4764413635323911361699183586	8415234243182787534123894858
1474343641823476922667154474	2267353254454872616182242154
2578649763684913163429325833	4689911847578741473186337883
5161596985226568681977938754	4428766787964834371794565542
2242632698981685551523361879	7146295186764167268433238125
7474189614567412367516833398	2273823813572968577469388278
6211855673345949471748161445	6686132721336864457635223349
4942716233498772219251848674	3161518296576488158997146221
5516264359672753836539861178	1917611425739928285147758625
5854762719618549417768925747	3516431537343387135357237754
5313691171963952518124735471	7549684656732941456945632221
6737691754241231469753717635	2397876675349971994958579984
4292388614454146728246198812	4675844257857378792991889317
4468463715866746258976552344	2832515241382937498614676246
2638621731822362373162811879	8755442772953263299368382378
1258922263729296589785418839	9833662825734624455736638328
4482279727264797827654899397	5298671253425423454611152788
8749855322285371162986411895	9857512879181186421823417538
1116599457961971796683936952	1471226144331341144787865593
3879213273596322735993329751	3545439374321661651385735599
9212359131574159657168196759	6735367616915626462272211264
3351223183818712673691977472	2141665754145475249654938214
8855835322812512868896449976	8481747257332513758286947416
4332859486871255922555418653	9961217236253576952797397966
2428751582371964453381751663	9941237996445827218665222824
6738481866868951787884276161	6242177493463484861915865966
8794353172213177612939776215	4344843511782912875843632652
2989694245827479769152313629	7568842562748136518615117797
6117454427987751131467589412	2776621559882146125114473423
2761854485919763568442339436	6174299197447843873145457215
6884214746997985976433695787	5387584131525787615617563371
8671829218381757417536862814	5317693353372572284588242963
9431156837244768326468938597	6612142515552593663955966562
4788448664674885883585184169	1314928587713292493616625427
3624757247737414772711372622	2446827667287451685939173534
9361819764286243182121963365	9786693878731984534924558138
9893315516156422581529354454	2926718838742634774778713813
5913625989853975289562158982	3791426274497596641969142899
8313891548569672814692858479	2831727715176299968774951996
2265865138518379114874613969	3281287353463725292271916883
3477184288963424358211752214	9954744594922386766735519674
6321349612522496241515883378	3414339143545324298853248718

\$1,000
Domino Program

d_1	d_2	d_3
0	01	110
100	00	11

$d_3d_1d_3 =$

110	0	110
11	100	11

$\longrightarrow$

1100110
1110011

Goal: Want same top and bottom.

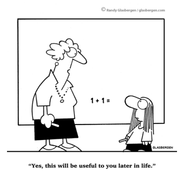
Domino program:

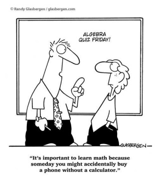
Input: dominos

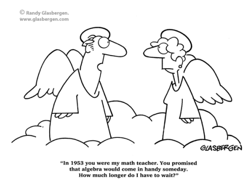
Output: sequence that works
or
say it can't be done

\$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: $F = \{f, o, x\}$; $V = \{a, e, i, o, u\}$.

$$F \cap V = \{o\} \qquad F \cup V = \{a, e, f, i, o, u, x\} \qquad \overline{F} = ?$$

2. natural numbers $\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$ What is "$\ldots$?"
   integers $\mathbb{Z} = \{0, \pm1, \pm2, \pm3, \pm4, \pm5, \ldots\}$

3. $E = \{2, 4, 6, 8, 10, 12, \ldots\}$ $\qquad E' = \{2, 4, 6, 8, 10, 13, \ldots\}$ What is "$\ldots$?"

4. $E = \{n \mid n = 2k;\ k \in \mathbb{N}\}$ $\leftarrow$ no "$\ldots$"

   Pop Quiz: Define $O = \{\text{odd numbers}\}$.

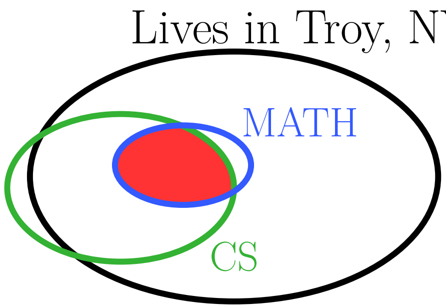
5. Rational numbers $\mathbb{Q} = \left\{r \,\middle|\, r = \frac{a}{b};\ a \in \mathbb{Z},\ b \in \mathbb{N}\right\}$

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

1. List of objects: order and repetition matter.

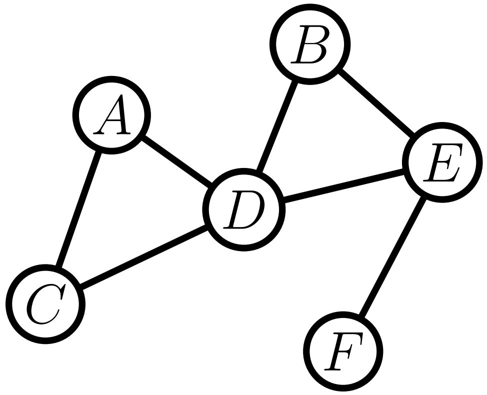
$$tap \neq taap \neq atp$$

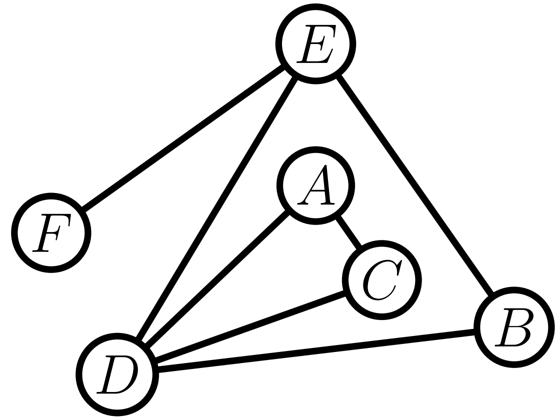
2. We are mostly concerned with *binary sequences* composed of *bits* (ASCII code).

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

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:

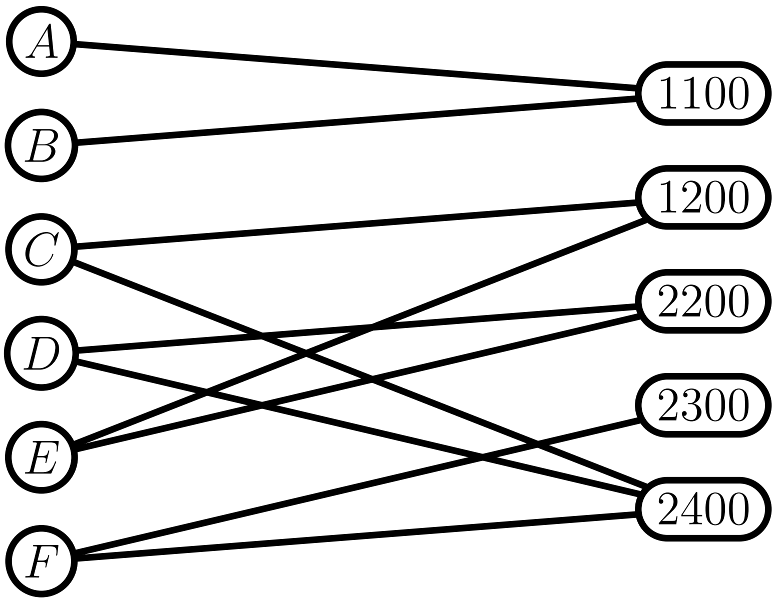
who the people are, that is the set V of objects; and,

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.

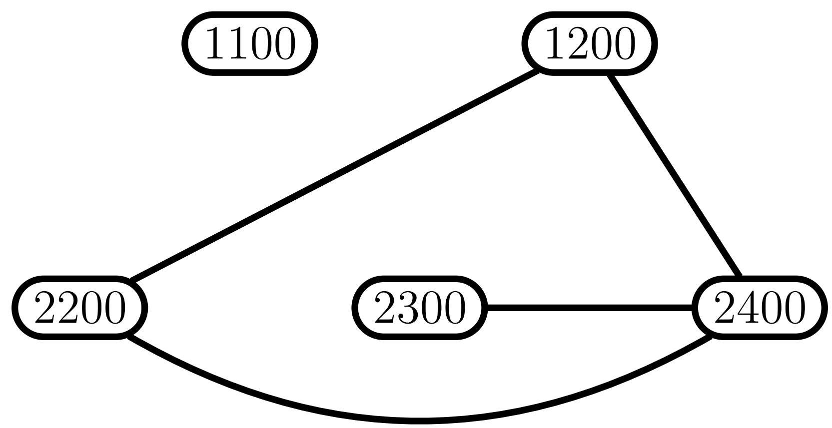
Graphs and Different Types of Relationships

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	$\ldots$
n^2	$\boxed{\mathbf{0}}$	1	$\boxed{\mathbf{4}}$	9	$\boxed{\mathbf{16}}$	25	$\boxed{\mathbf{36}}$	49	$\boxed{\mathbf{64}}$	81	$\boxed{\mathbf{100}}$	121	$\ldots$

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) $\underline{n \text{ is even}} \rightarrow\ n = 2k\ \rightarrow\ n^2 = 2(2k^2)\ \rightarrow\ n^2$ **is even**.

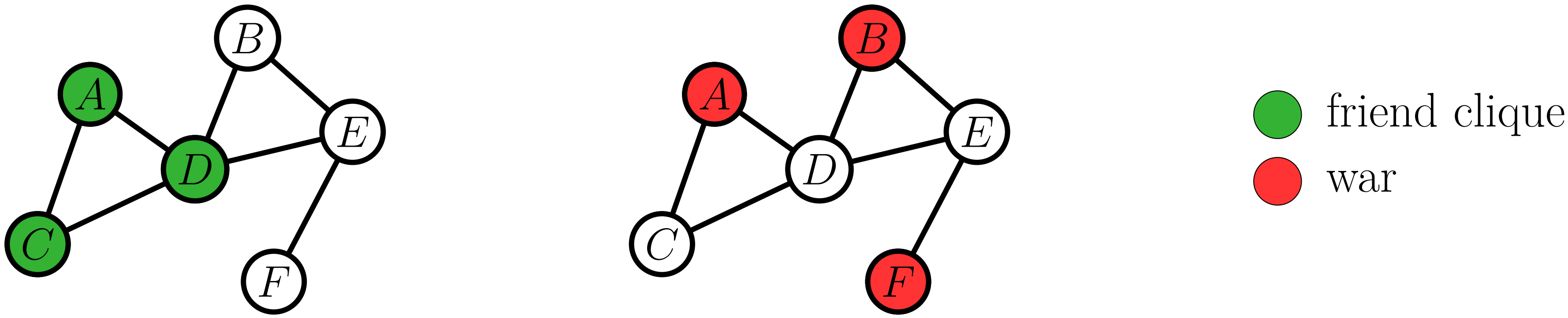
(ii) $\underline{n \text{ is odd}} \rightarrow\ n = 2k+1\ \rightarrow\ n^2 = 2(2k^2+2k)+1\ \rightarrow\ n^2$ **is odd**.

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.

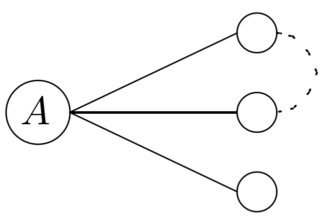
3-war or 3-clique



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:

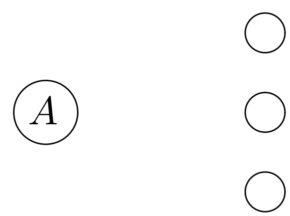
(i) A has more friends than enemies.



Two friends are linked → 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 $\mathbb{N} = \{1, 2, 3, \ldots\}$ has a minimum element.

$$\{2, 5, 4, 11, 7, 296, 81\}; \text{ or,}$$
$$\{6, 19, 24, 18, \ldots\}.$$

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,

$$\boxed{\sqrt{2}} = \left\{\frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}, \frac{a_4}{b_4}, \ldots\right\},$$

$\leftarrow$ all possible ways to write $\sqrt{2}$ as a fraction

where $a_1, a_2, \ldots$ are all integers and $b_1, b_2, \ldots$ 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.**

FISHY!

Reductio ad Absurdum

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.