

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)

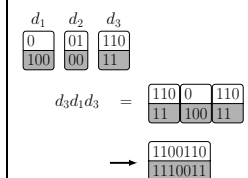
\$100

Distinct subsets with the same sum.

57198259597961340554155629
34879408284115806672137984
4767390177454742284770314
185392491979773212586239784
42697784124089795151647977
796713896179884808409417196
257296779661319022764888
1285874181925830860381981
47641383528138109185496
1474348418241700296714474
27764673661911324829293
561198865266868197738754
22832839089885915283849
74743984166741286175683398
62138587334949471748161445
84871824398772105848674
5516364967478383628861178
5854925198498491788026747
53189117963951813175471
67270371424123116075711305
42828981441462284198812
4684807158687462587032344
263807174328271748811879
1258922672925964978418839
4822797273647979264489397
874852226257118296411866
114659815796197179683936952
3876311875862275982329714
9212559137419657168196759
35122318381871867899197472
88582828261612688848976
43285948871852255448653
24257182375644613817660
67848186868686912578842563
879435172911781289778215
298984848474797015131329
61174544798775118186789412
2761544809170365846233948
68621414897786164809787
80718291188175711738862814
942158674142836848883957
4784486687488588581844409
3024737217741477271173622
90818197429621311412196362
98831516456424812854454
5913228898387786860318982
8318915486967281460285479
2282661381879911874812809
187184898644145811752214
6218496132249824151888378

\$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

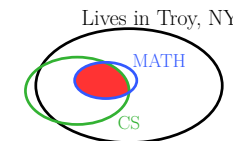
- Sets
- Sequences
- Graphs

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

- Collection of objects, order does not matter: $F = \{f, o, x\}$; $V = \{a, e, i, o, u\}$.
 $F \cap V = \{o\}$ $F \cup V = \{a, e, f, i, o, u, x\}$ $\bar{F} = ?$
- 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 "...?"
- $E = \{n \mid n = 2k; k \in \mathbb{N}\}$ ← 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, \bar{A}
- Venn Diagrams are a convenient way to represent sets.



Sequences

- 1 List of objects: order and repetition matter.

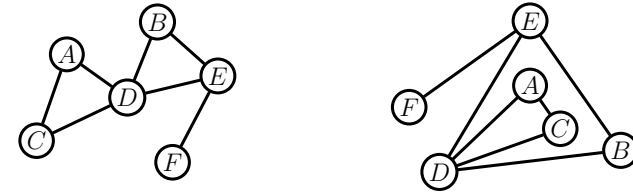
$$tap \neq taap \neq atp$$

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

$$\begin{array}{ccc} t & a & p \\ 01110100 & 011100001 & 011110000 \end{array}$$

Graphs

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



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

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

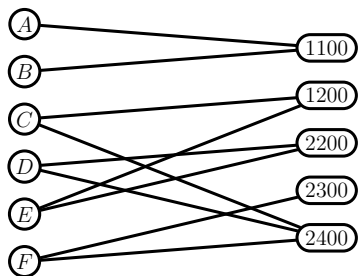
What matters is:

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.

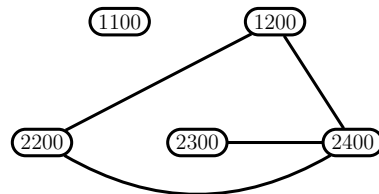
Graphs and Different Types of Relationships

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 has risen every morning in history. (*inductive proof*)

- 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 is 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*

● n is even $\rightarrow n = 2k \rightarrow n^2 = 2(2k^2) \rightarrow n^2$ is even.

● n is odd $\rightarrow n = 2k + 1 \rightarrow n^2 = 2(2k^2 + 2k) + 1 \rightarrow n^2$ is odd.

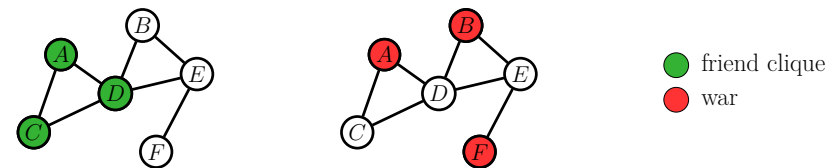
n must be even or odd, and we made no assumptions about n (n is *general*).

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



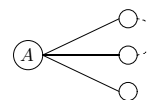
Theorem.

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.

(ii) A has more enemies than friends.



Two friends are linked \rightarrow 3-clique.

Two friends are enemies \rightarrow 3-war.

None are linked \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} has a minimum element.

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

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 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.