

Discrete Objects



- Malik Magdon-Ismael. Discrete Mathematics and Computing.
 - Chapter 2

- Discrete Objects
 - Sets
 - Sequences
 - Graphs
- 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

- Collection of objects without duplicates, order does not matter:

$$F = \{f, o, x\} = \{f, f, o, x\}$$

$$V = \{a, e, i, o, u\}$$

$$\emptyset = \{\}$$

$$F \cap V = ?; F \cup V = ?$$

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

$$\bar{F} = \{x \mid x \notin F\} = ? \text{ (trick question)}$$

$$\bar{F} = \{a, e, i, u\} \quad (\text{assuming universe is } F \cup V)$$

- Famous sets

- natural numbers $\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}$

- integers $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$

- What is “...?”

- You should provide enough information so that it is clear

$$E = \{2, 4, 6, 8, 10, 12, \dots\}$$

14, 16, ...

$$E' = \{2, 4, 6, 8, 10, 13, \dots\}$$

huh?



- Can define sets without " ... "

$$E = \{n \mid n = 2k; k \in \mathbb{N}\}$$

- What is E ?
- All even numbers, i.e., $E = \{2, 4, 6, \dots\}$

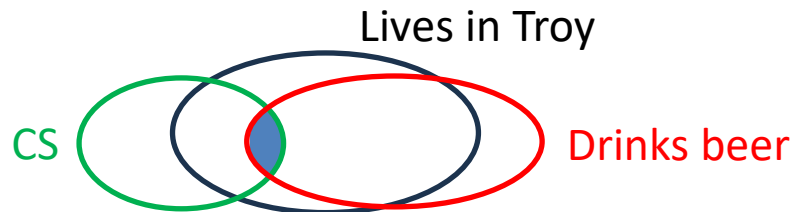
- Can define sets without " ... "

$$E = \{n \mid n = 2k; k \in \mathbb{N}\}$$

- What is E ?
- All even numbers, i.e., $E = \{2, 4, 6, \dots\}$
- Rational numbers $\mathbb{Q} = \left\{r \mid r = \frac{a}{b}, a \in \mathbb{Z}, b \in \mathbb{N}\right\}$
- Subset $A \subseteq B$
 - every element of A is in B

$$\emptyset \subseteq A, \text{ for any } A$$

- Power set $\mathcal{P}(A) = \{\text{all subsets of } A\}$
- Suppose $A = \{a, b\}$. What is $\mathcal{P}(A)$?
$$\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$$
- 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



- List of objects: order and repetition matter

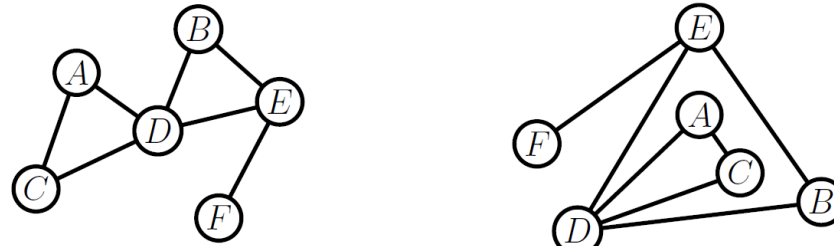
tap ≠ *taap* ≠ *atp*

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

t
a
p
 01110100 01100001 01110000

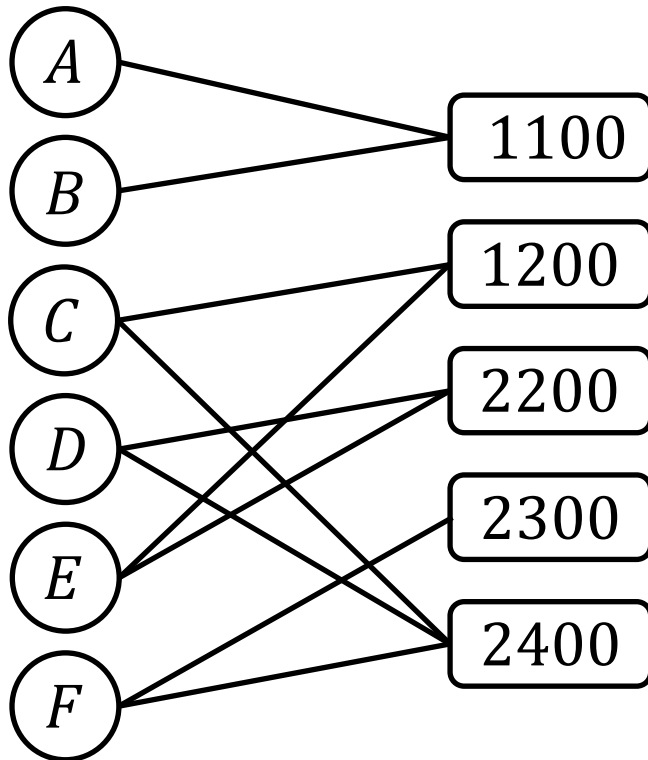
dec	hex	oct	char	dec	hex	oct	char	dec	hex	oct	char	dec	hex	oct	char
0	0	000	NULL	32	20	040	space	64	40	100	@	96	60	140	`
1	1	001	SOH	33	21	041	!	65	41	101	A	97	61	141	a
2	2	002	STX	34	22	042	"	66	42	102	B	98	62	142	b
3	3	003	ETX	35	23	043	#	67	43	103	C	99	63	143	c
4	4	004	EOT	36	24	044	\$	68	44	104	D	100	64	144	d
5	5	005	ENQ	37	25	045	%	69	45	105	E	101	65	145	e
6	6	006	ACK	38	26	046	&	70	46	106	F	102	66	146	f
7	7	007	BEL	39	27	047	'	71	47	107	G	103	67	147	g
8	8	010	BS	40	28	050	(72	48	110	H	104	68	150	h
9	9	011	TAB	41	29	051)	73	49	111	I	105	69	151	i
10	a	012	LF	42	2a	052	*	74	4a	112	J	106	6a	152	j
11	b	013	VT	43	2b	053	+	75	4b	113	K	107	6b	153	k
12	c	014	FF	44	2c	054	,	76	4c	114	L	108	6c	154	l
13	d	015	CR	45	2d	055	-	77	4d	115	M	109	6d	155	m
14	e	016	SO	46	2e	056	.	78	4e	116	N	110	6e	156	n
15	f	017	SI	47	2f	057	/	79	4f	117	O	111	6f	157	o
16	10	020	DLE	48	30	060	0	80	50	120	P	112	70	160	p
17	11	021	DC1	49	31	061	1	81	51	121	Q	113	71	161	q
18	12	022	DC2	50	32	062	2	82	52	122	R	114	72	162	r
19	13	023	DC3	51	33	063	3	83	53	123	S	115	73	163	s
20	14	024	DC4	52	34	064	4	84	54	124	T	116	74	164	t
21	15	025	NAK	53	35	065	5	85	55	125	U	117	75	165	u
22	16	026	SYN	54	36	066	6	86	56	126	V	118	76	166	v
23	17	027	ETB	55	37	067	7	87	57	127	W	119	77	167	w
24	18	030	CAN	56	38	070	8	88	58	130	X	120	78	170	x
25	19	031	EM	57	39	071	9	89	59	131	Y	121	79	171	y
26	1a	032	SUB	58	3a	072	:	90	5a	132	Z	122	7a	172	z
27	1b	033	ESC	59	3b	073	;	91	5b	133	[123	7b	173	{
28	1c	034	FS	60	3c	074	<	92	5c	134	\	124	7c	174	
29	1d	035	GS	61	3d	075	=	93	5d	135]	125	7d	175	}
30	1e	036	RS	62	3e	076	>	94	5e	136	^	126	7e	176	~
31	1f	037	US	63	3f	077	?	95	5f	137	_	127	7f	177	DEL

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



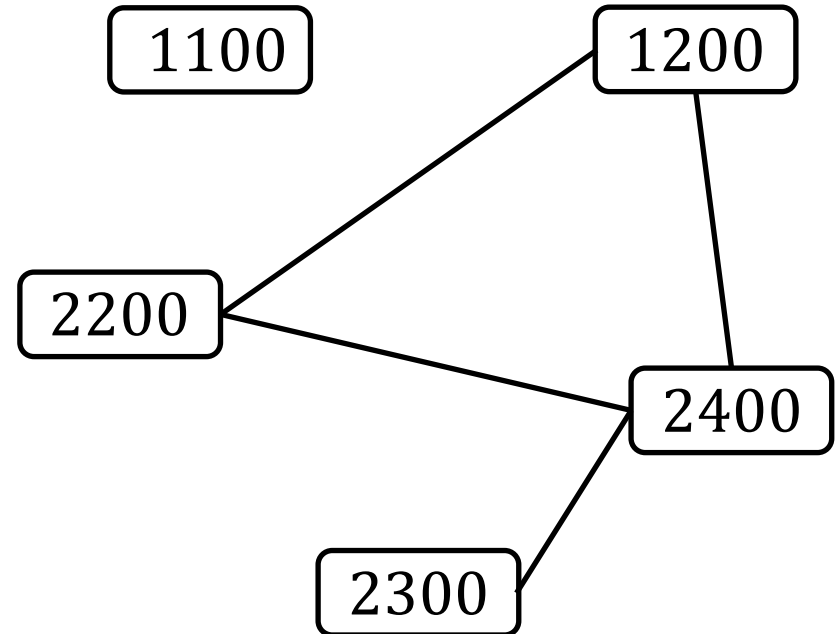
- Each vertex/node in the graph corresponds to a person
$$V = \{A, B, C, D, E, F\}$$
- Each edge between nodes means those people are friends
$$E = \{(A, C), (A, D), (C, D), (D, B), (D, E), (B, E), (E, F)\}$$
- Graph has no “orientation”. What matters is:
 - who the people are, that is the set V of objects; and,
 - who is friends with whom, that is the set E of relationships.
- The picture with circles and links is a convenient *visualization*

- Affiliation graphs



Students and their courses

- Conflict graphs



Courses with students in
common conflict (why?)
Same student in both

- 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:
 - At most how many people can a person meet in any round? Why?
 - In any round a person meets at most 3 new people (4 per table)
 - 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
 - Don't get too confident, though
 - People make mistakes, especially if it's a new proof
 - Computer-checked theorem proofs exist for a reason
 - A whole field of CS is concerned with encoding your pen-and-paper proofs into a programming language that can check if your proof is correct

When is a number a square?



- Before we prove anything, think about what squares look like

$$n = \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 7$$
$$n^2 = 1, 4, 9, 16, 25, 36, 49$$

- **Conjecture:** *Even squares come from even numbers*

- **Proof** (How do I convince you?):

- First look at even n

- By definition, $n = 2k$ for some integer k

- $n^2 = 4k^2$

- (is this even?)

- Yes, $n^2 = 2(2k^2)$

- How about odd n ?

$$n = 2k + 1$$
$$n^2 = 4k^2 + 4k + 1$$
$$= 2(2k^2 + 2k) + 1$$

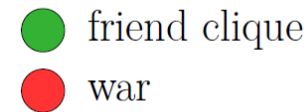
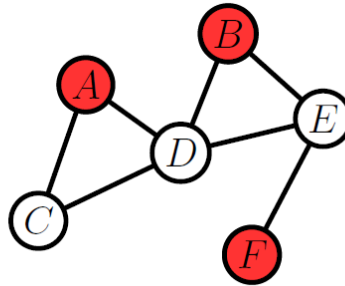
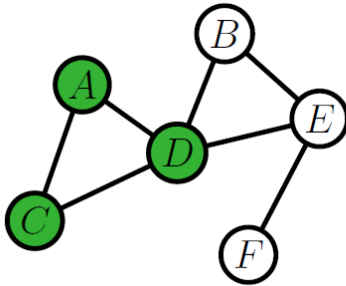
When is a number a square?, cont'd



- **Conjecture:** *Even squares come from even numbers*
- **Proof** (How do I convince you?):
 - Even numbers \rightarrow even squares
 - Odd numbers \rightarrow odd squares
 - Every number is either even or odd
 - Every even square must come from a number
 - Every number is either even or odd
 - It cannot be the case that an even square came from an odd number because all odd numbers produce odd squares
 - 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

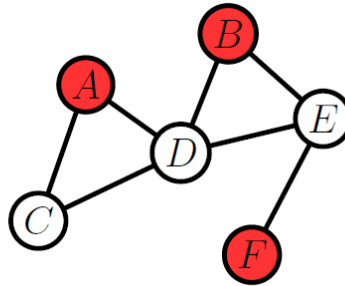
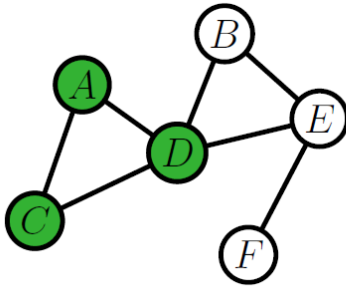
- Look at these friendship graphs



- **Theorem:** Any 6-person friend network, has a 3-person friend clique or a 3-person war (or both)
- Before we prove it: who cares?
 - At every party, you either have a big clique of friends
 - Or there's conflict!
 - In the world, there are either big coalitions or big groups of enemies
 - Assuming two countries are either friends or enemies

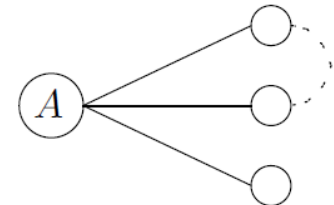
3-war or 3-clique

- Look at these friendship graphs



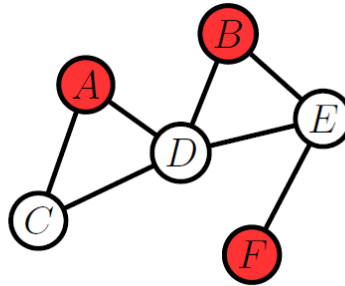
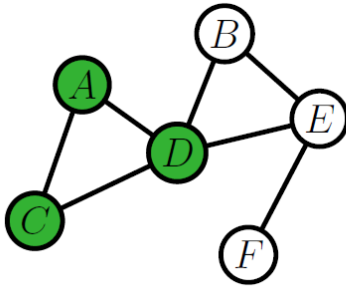
● friend clique
● war



- **Theorem:** Any 6-person friend network, has a 3-person friend clique or a 3-person war (or both)
- **Proof:**
 - Case 1: person A has more friends than enemies
 - At least how many friends does A have?
 - Case 1.A: At least two of A 's friends are friends
 - We have a 3-clique
 - Case 1.B: None of A 's friends are friends
 - We have a 3-war



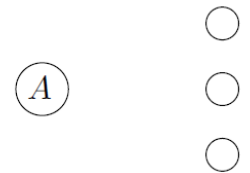
3-war or 3-clique

- Look at these friendship graphs



 friend clique
 war

- Theorem:** Any 6-person friend network, has a 3-person friend clique or a 3-person war (or both)
- Proof:**
 - Case 2: person A has more enemies than friends
 - How many enemies does A have at least?
 - At least 3
 - Case 2.A: All three are friends (3-clique)
 - Case 2.B: At least two are enemies (3-war, counting A)



- **Axioms:** A self-evident statement that is asserted as true without proof
 - Building blocks of proofs
 - Can't prove anything without axioms!
 - Any proof is an application of some rule given the axioms
 - E.g., deduction, induction
 - All mathematical theories are essentially sets of axioms
 - Most popular theory of the real numbers is the Zermelo-Fraenkel theory with the Axiom of Choice (ZFC)
- **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

- Turns out the world of numbers can be quite complex
- Need some fairly non-obvious axioms
- **Axiom** [*The Well-Ordering Principle (also known as the Axiom of Choice)*]:
 - Any non-empty subset of $\mathbb{N} = \{1, 2, 3, \dots\}$ has a minimum element
 - Finite $\{2, 5, 4, 11, 7, 296, 81\}$
 - Infinite $\{6, 19, 24, 18, \dots\}$
- This is an axiom because we can't prove it from the other axioms
 - But it's necessary for more interesting proofs
 - E.g., prime number factorization

- Construct a subset of \mathbb{Z} (integers) that has no minimum element
 - E.g., $S = \{-1, -2, -3, \dots\}$
- Construct a positive subset of \mathbb{Q} (rationals) that has no minimum element
 - E.g., $S = \left\{1, \frac{1}{10}, \frac{1}{100}, \dots\right\}$
 - Why does this set have no minimum?
 - Give me any $a \in S$
 - We know $a > 0$
 - There exists some power of 10, p , such that $a > \frac{1}{10^p}$

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



- Irrational means $\sqrt{2}$ is not a member of \mathbb{Q}
- We will prove this using a proof by contradiction
 - Assume the opposite and show it leads to an impossibility
- Assume $\sqrt{2}$ is rational
 - What does this imply?
 - There exist an integer p and a natural number q such that $\sqrt{2} = \frac{p}{q}$
 - Note that p and q may not be unique
 - E.g., $2 = \frac{2}{1} = \frac{4}{2} = \frac{6}{3} = \dots$
 - Let $R = \left\{ \frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3}, \dots \right\}$ be all ways in which we can write $\sqrt{2}$
 - Let $q_* \in R$ be the smallest q_i
 - Why does q_* exist?
 - Well-Ordering Principle!

A Gift from Hipassus: $\sqrt{2}$ is irrational, cont'd

- Assume $\sqrt{2}$ is rational
 - Let $R = \left\{ \frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3}, \dots \right\}$ be all ways in which we can write $\sqrt{2}$
 - Let $q_* \in R$ be the smallest q_i
 - Why does q_* exist?
 - Well-Ordering Principle!
 - Let p_* be the corresponding p_i
- Note that p_* and q_* have no factor in common
 - Why?
 - Because q_* was the smallest possible
 - For any other p_j, q_j pair, it must be the case that $\frac{p_j}{q_j} = \sqrt{2} = \frac{kp_*}{kq_*}$
- Raise both sides of $\sqrt{2} = \frac{p_*}{q_*}$ to power 2
$$2q_*^2 = p_*^2$$
 - This means p_*^2 is even (hence p_* is even), i.e., $p_* = 2k$ for some $k \in \mathbb{N}$
 - Then, $2q_*^2 = 4k^2 \rightarrow q_*^2 = 2k^2$ **q_* is also even!**

A Gift from Hipassus: $\sqrt{2}$ is irrational, cont'd



- Assume $\sqrt{2}$ is rational
 - Let $R = \left\{ \frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3}, \dots \right\}$ be all ways in which we can write $\sqrt{2}$
 - Let $p_* \in R$ be the smallest p_i
 - Why does p_* exist?
 - Well-Ordering Principle!
 - Let q_* be the corresponding q_i
- Note that p_* and q_* have no factor in common
 - Why?
 - Because p_* was the smallest possible
- Both p_* and q_* are even
 - Contradiction
 - Why?
 - I just told you they have no factor in common
 - But that implies they have a factor of 2 in common
 - QED

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**
- Even experienced mathematicians skip steps and confuse themselves sometimes

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.
- **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.