Recitation Notes

H241: Discrete Structures

Spring Term 2025

1/17/2025

Recitation held over Zoom with Prof. Leivant (I was out of town). Notes are available on the Course Material page.

1/24/2025

The plan for today:

- Check in, how are you all doing?
- Homework questions
- Talk about different proof strategies

Let's take a pause from sets and relations for a moment. For most of you, this is probably the first maths class where you've been expected to prove claims from scratch. We expect your proofs to look pretty much like what you've seen in class and on the solved homework examples. Any logically sound argument from premise to goal counts as a proof. It's good to write in a conversational tone, but at least in the beginning it's important to show every step, and make sure each sentence logically follows the previous one.

We will take a moment now to review the different types of proofs we've seen:

Proof by Construction / Example. If you are asked to show "there exists some X with property P(X)" (or "there is", or "define"), then all you need to do is *give a construction / give an example*! It's important to make sure to check that P(X) is actually true.

- **Example:** Show that there are primes p, q that are twin primes, i.e. $|p - q| = 2$.
  Proof: 3 and 5 are twin primes. We can check: $|3 - 5| = 2$ ✔

Similarly, if you're asked to show "not every X has property P(X)", all you need to do is *give a counterexample*, and check that P(X) holds for that counterexample.

Direct Proof. If you're asked to show "every X has property P(X)", then pick an arbitrary X (all you can assume about it is given by its definition), then show that P(X) holds. The same principle applies when proving implications "if X then Y"—suppose X, then prove Y.

- **Example:** Show that all primes $p > 2$ are odd.
  Proof: Let $p > 2$ be prime. By definition of prime, p's only divisors are p and 1. In particular, none of its divisors are 2. So p must be odd.

Proof by Contradiction.

- **Example:** Show that all primes $p > 2$ are odd.
  Proof: Let $p \geq 2$ be prime, and suppose for contradiction that it's even. That is, $p = 2m$ for some integer $m > 0$. We have two cases:

***m* = 1.** So $p = 2$. But $p > 2$ (a contradiction!)

***m* > 1.** So p is divisible by 2 and some $m > 1$. But this contradicts the fact that p is prime.

Prof. Leivant (and many computer scientists) prefer to avoid proofs by contradiction because they aren't *constructive*, i.e. they don't show you how to actually get to the conclusion from the premise.

Proof by Cases. The above proof also demonstrates a "proof by cases". If our goal is to prove X, we can choose to split into cases. So long as we cover all possible cases (e.g. we consider both P and not-P, or we consider $m = 1, m < 1, m > 1$, etc.), and prove X in each case, we have proven X in general. In general, this proof technique is also not constructive.

Proof by Contraposition. Here's a general logical principle which we take as sound: X implies Y iff *not*-Y implies *not*-X. Sometimes it's easier to prove that not-Y implies not-X! (Note that in general, this proof technique is also not constructive.)

- **Example:** If r is irrational, then $r^{\frac{1}{5}}$ is irrational.

  Proof: Let's prove the contrapositive: If $r^{\frac{1}{5}}$ is rational, then r is rational. Suppose $r^{\frac{1}{5}}$ is rational, i.e. $r^{\frac{1}{5}} = \frac{a}{b}$ where a, b are integers and $b \neq 0$. So

  $$r = \left(r^{\frac{1}{5}}\right)^5 = \left(\frac{a}{b}\right)^5 = \frac{a^5}{b^5}$$

  Since a is an integer, so is a^5, and similarly for b. So r is rational.

In class we showed that $\sqrt{2}$ is irrational. Let's put all these techniques together to show:

Proposition. There exist irrational numbers a, b such that a^b is rational.

Proof. Instead of actually giving a and b, we can (nonconstructively) split into two cases, and in each case find a different a^b. (This proof is cute, but unsatisfying in the sense that we never really say which world we're actually in. This is one reason why many computer scientists prefer constructive/direct proofs).

Case 1. $\sqrt{2}^{\sqrt{2}}$ is rational. In this case, let $a = \sqrt{2}, b = \sqrt{2}$. We have $a^b = \sqrt{2}^{\sqrt{2}}$, which is rational.

Case 2. $\sqrt{2}^{\sqrt{2}}$ is irrational. In this case, let $a = \sqrt{2}^{\sqrt{2}}$, and let $b = \sqrt{2}$. We have

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\sqrt{2}} = \sqrt{2}^2 = 2$$

which is rational.

□

1/31/2025

This week in class we talked about counting, countable numbers, invariants, and reasoning by induction. The plan for today:

- Check in, how are you all feeling? Are we going too fast?
- Homework questions
- Talk about the fact that real numbers are not countable.

On Tuesday, we formalized the common idea that "some infinities are bigger than other infinities." Many infinite sets, such as $\mathbb{N}, \mathbb{Z}, \mathbb{N} \times \mathbb{N}$, and $\mathbb{Q}^+$ are *countable* because they can be put in one-to-one correspondence (bijection) with the natural numbers $\mathbb{N}$. But many infinite sets are *not* countable. In class, we showed that $\mathcal{P}(\mathbb{N})$ is not countable. Actually, we showed the much more general theorem proved by Georg Cantor in 1891 that *any* set $\mathcal{P}(A)$ can't be put in one-to-one correspondence with A. (Think of $\mathcal{P}(A)$ as "strictly larger" than A—which formally means that $\mathcal{P}(A) \not\leq A$; equivalently, there is no injection from $\mathcal{P}(A)$ into A; equivalently, there is no surjection from A into $\mathcal{P}(A)$.

We mentioned that the real numbers $\mathbb{R}$ are *also* uncountable. But how can we prove it? To make our lives easier, consider a smaller part of the real number line, say $(0, 1)$. If there *was* a bijection from $\mathbb{N}$ to $\mathbb{R}$, then there certainly would be one from $\mathbb{N}$ to $(0, 1)$. So it's enough to show that $(0, 1)$ is uncountable. Okay, but how do we define $(0, 1)$? One way is to define $(0, 1)$ as the set of all numbers of the form

$$0.a_1a_2a_3a_4\ldots$$

where $a_1, a_2, a_3, a_4, \ldots$ are digits between 0 and 9. One potential issue is that a real number can have multiple equivalent decimal expansions, e.g.

$$0.4999\ldots = 0.5000\ldots$$

But we can resolve this by supposing real numbers are in a certain "canonical form", e.g. in the case above we suppose the number is in the form $0.5000\ldots$ with trailing 0's instead of trailing 9's.

Theorem. The real interval $(0, 1)$ is uncountable.

Proof. Suppose for contradiction that it is countable. Intuitively, this means there is some way to "count" all the reals within $(0, 1)$ without missing any of them. Formally, we say there is a surjection

$$f : \mathbb{N} \to (0, 1)$$

f "counts" by associating every natural number with some real in $(0, 1)$. Because f is surjective, it doesn't miss any of them. So we have the mapping:

$$\begin{array}{lll} 0 & \to & 0.a_{11}a_{12}a_{13}a_{14}a_{15}\ldots \\ 1 & \to & 0.a_{21}a_{22}a_{23}a_{24}a_{25}\ldots \\ 2 & \to & 0.a_{31}a_{32}a_{33}a_{34}a_{35}\ldots \\ 3 & \to & 0.a_{41}a_{42}a_{43}a_{44}a_{45}\ldots \\ 4 & \to & 0.a_{51}a_{52}a_{53}a_{54}a_{55}\ldots \\ \ldots & \ldots & \ldots \end{array}$$

and so on. I will now contradict our hypothesis by constructing a real number, in $(0, 1)$, that is not in this list! Let b be the number $b = 0.b_1b_2b_3b_4b_5\ldots$ whose digits are

$$b_i = \begin{cases} 0 & \text{if } a_{ii} \neq 0 \\ 1 & \text{otherwise} \end{cases}$$

For example, if we have the mapping

$$\begin{array}{lll} 0 & \to & 0.\mathbf{9}3201\ldots \\ 1 & \to & 0.7\mathbf{3}055\ldots \\ 2 & \to & 0.08\mathbf{0}12\ldots \\ 3 & \to & 0.001\mathbf{0}1\ldots \\ 4 & \to & 0.9999\mathbf{9}\ldots \\ \ldots & \ldots & \ldots \end{array}$$

then $b = 0.00110$. In general, we're going along the diagonal and making each i^{th} digit of b to be exactly **not** the i^{th} digit of the i^{th} listed number. By construction, b cannot be the number $f(0)$, nor the number $f(1)$, nor the number $f(2)$, and so on. By an inductive argument, b cannot be any of the listed numbers, which means f is not a surjection (a contradiction!) □

Question. Which do you think is larger, $\mathbb{R}$, or $\mathcal{P}(\mathbb{N})$? (If you're up for a challenge—prove it!)

2/7/2025

Let's do more induction practice!

Example 1. Prove that $3^n > n^2$ for all integers $n \geqslant 1$.

Note. You can assume that $n^2 \geqslant 2n$ for all $n \geqslant 1$, or otherwise just prove it seperately by induction.

Proof. By induction on n.

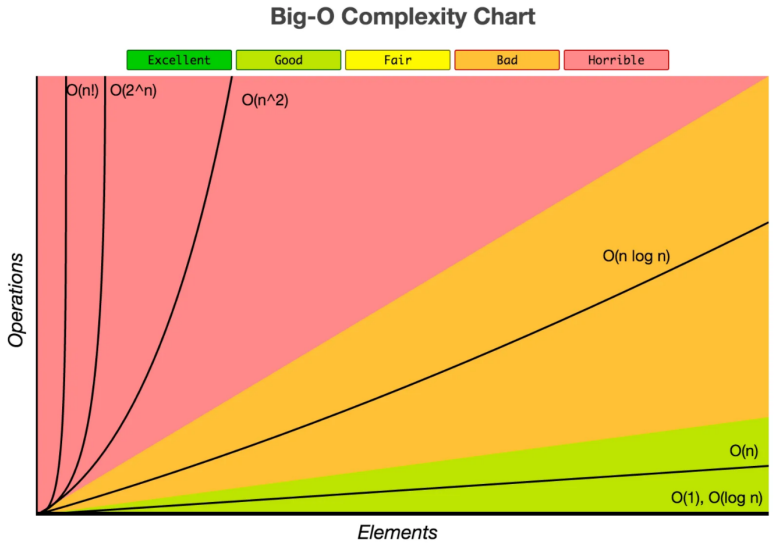
Base. $n = 1$. In this case, we have $3^n = 3^1 = 3 > 1 = 1^2 = n^2$. ✔

Induction Step. Let $n \geqslant 1$, and suppose our inductive hypothesis, i.e., $3^n > n^2$. We now need to show that this holds for the next step $n+1$, i.e. $3^{n+1} > (n+1)^2$. Well,

$$\begin{aligned}
3^{n+1} &= 3 \cdot 3^n && \text{(pull out the 3)} \\
&> 3 \cdot n^2 && \text{(apply our IH)} \\
&= n^2 + n^2 + n^2 \\
&\geqslant n^2 + 2n + n^2 && \text{(since } n^2 \geqslant 2n\text{)} \\
&\geqslant n^2 + 2n + 1 && \text{(since } n^2 \geqslant 1 \text{ for all } n \geqslant 1\text{)} \\
&= (n+1)^2
\end{aligned}$$

□

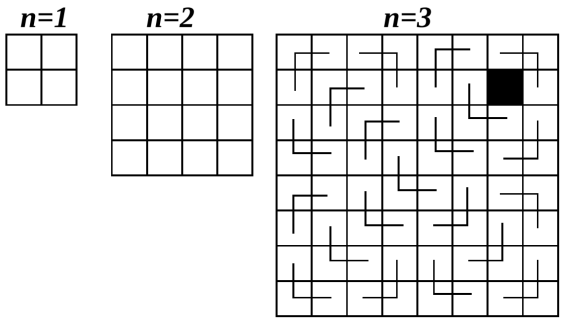
Question. Actually, $3^n > n^2$ for all integers $\boldsymbol{n \geqslant 0}$! How should we modify the proof above?



Example 2. Take a chessboard of size $2^n \times 2^n$, then remove one square. Prove that this board can be covered by trominos, i.e., 3-piece dominos that look like this:

Note. Let's look at some examples first. For $n = 1$ we have a 2×2 board; for $n = 2$ we have a 4×4 board, and for $n = 3$ we have an 8×8 board. Let's see how we can cover them with trominos:

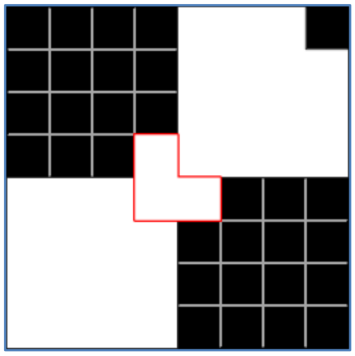
[source]



Proof. Let's try to prove this by induction on n.

Base. $n = 1$, and so we have the 2×2 board above. After we remove any square, it's easy to cover the remaining board with a single tromino.

Induction Step. Let $n \geqslant 1$, and suppose that after removing a square we can cover a board of size $2^n \times 2^n$ with trominos. Now consider a $2^{n+1} \times 2^{n+1}$ size board, and remove a square anywhere. Notice that this board is just 4 copies of $2^n \times 2^n$ boards, arranged in a square. Here's the trick—place a single tromino in the middle of this larger board, so that its inner edge is facing towards the square we removed:



The three squares touching the tromino are $2^n \times 2^n$ boards with one square removed, so they can be covered (by our IH!). And the remaining square is *also* a $2^n \times 2^n$ board with one square removed. So it can also be covered using our IH. So the whole board can be covered, and we're done. □

2/14/2025

This week in recitation we took the first test.

2/21/2025

We've covered a lot since 2 weeks ago! So I'll just give you all practice with combinatorics, probability, and graphs.

Problems.

1. What is the coefficient of x^3y^4 in the expansion of $(x+y)^7$?
2. What is the coefficient of x^2 in the expansion of $(x-2)^6$?
3. Suppose license plates consist of letters and digits of the form _ _ _ - _ _ _, how many different license plates are possible?
4. How many plates are there with no repeated symbols?
5. Adam sees patterns in license plates. How many license plates contain the consecutive letters "OBEY"?
6. Adam is particularly fixated on the pattern "143" (Mr. Rogers maintained his weight at 143, since it matches the number of letters within "I love you." [source]). How many license plates contain 143 (in that order, but not necessarily consecutive)?
7. Assuming a uniform distribution of license plates throughout the day, what is the probability of the two license plate events above?
8. Bob flips 2 fair coins. Alice flips 3. What is the probability that Alice gets strictly more heads than Bob?

   Hint: It helps if you first write down the sample space S, and the event E we're after.

Solutions.

1. In class we derived the Binomial Theorem, which says

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k}y^k$$

   (This is important enough to memorize, if you haven't already!) For $(x+y)^7$, $n=7$, and in the x^3y^4 term, $k=4$. The coefficient of this term is:

$$\binom{7}{4} = \frac{\mathbf{7!}}{\mathbf{4!(7-4)!}} = \frac{7\cdot6\cdot5\cdot4\cdot3\cdot2\cdot1}{(4\cdot3\cdot2\cdot1)(3\cdot2\cdot1)} = \frac{7\cdot6\cdot5}{3\cdot2\cdot1} = \mathbf{35}$$

2. For $(x-2)^6$, take $y=-2$ and $n=6$. Be careful here—since $x^2 = x^{6-4}$, we're actually looking at the term for $k=4$:

$$\binom{6}{4} x^{6-4}(-2)^4$$

   So the coefficient is actually $\binom{6}{4}\cdot(-2)^4$. Let's calculate this out:

$$\binom{6}{4}\cdot(-2)^4 = \frac{\mathbf{6!}}{\mathbf{4!(6-4)!}}\cdot\mathbf{16} = \frac{6\cdot5}{2}\cdot16 = \mathbf{240}$$

3. The total number of symbols is $26+10=36$ (letters and digits). For each symbol S, we have 36 options. So the total number is $36\cdot36\cdot36\cdot36\cdot36\cdot36 = \mathbf{36^6}$ (=2176782336).

4. For the first symbol, we have 36 options, then 35 options, and so on. The total number is

$$36 \cdot 35 \cdot 34 \cdot 33 \cdot 32 \cdot 31 = \frac{\mathbf{36!}}{\mathbf{(36-6)!}} \, (=1402410240)$$

5. The basic idea is to treat "OBEY" like a fixed block. First, we should count the number of ways to position this block:

```
O B E - Y _ _
_ O B - E Y _
_ _ O - B E Y
```

Fortunately we don't have to worry about the other letters contributing to another "OBEY", and so there is no overlap between these possibilities. There are 3 possible positions of "OBEY", and in each of these cases we have $36 \cdot 36$ options for the remaining symbols. So the total number of license plates is

$$\mathbf{3 \cdot 36 \cdot 36} \, (=3888)$$

6. Since the order of the symbols $1,4,3$ is fixed, we really just need to pick 3 arbitrary positions for them to fall in. For example, here is one possible position:

```
_ 1 _ - 4 3 _
```

Note that the order in which we choose *these positions* does not matter—we're just picking 3 positions! What is the number of ways to pick 3 positions from 6, when order doesn't matter? It's just $\binom{6}{3}$!

Picking the remaining symbols is now easy. We have $36 \cdot 36 \cdot 36$ options (since order matters, and they are not necessarily unique). The total number of license plates is:

$$\mathbf{\binom{6}{3} \cdot 36 \cdot 36 \cdot 36} \, (=933120)$$

7. The sample space is $S = \{$_ _ _ - _ _ _$|$ the entries are $\in$ A-Z and 0-9$\}$. The size of this space is just the number of license plates $|S| = 36^6$. Since the space is uniformly distributed, the probability of observing any particular license plate a is $P(a) = \frac{1}{36^6}$.

The first event is $E_1 = \{$_ _ _ - _ _ _$|$ it contains the consecutive letters "OBEY"$\}$. The size of this event is $|E_1| = 3 \cdot 36 \cdot 36$, so the probability of the event is

$$P(E_1) = \sum_{a \in E_1} P(a) = \frac{\mathbf{3 \cdot 36 \cdot 36}}{\mathbf{36^6}} \approx 0.000179\,\%$$

The second event is $E_2 = \{$_ _ _ - _ _ _$|$ it contains 1,4,3, in that order$\}$. The size of this event is $|E_2| = \binom{6}{3} \cdot 36 \cdot 36 \cdot 36$, so the probability of the event is

$$P(E_2) = \sum_{a \in E_2} P(a) = \frac{\mathbf{\binom{6}{3} \cdot 36 \cdot 36 \cdot 36}}{\mathbf{36^6}} \approx 0.043\,\%$$

8. The sample space here is $S =$ the set of coin flip sequences—to separate Bob's from Alice's, let's write them as (for example) HT-HTT. The event that Alice gets strictly more heads than Bob is the set:

$$E = \{\text{HH-HHT}, \text{HH-THH}, \text{HH-HTH}, \text{HT-HHH}, \dots\}$$

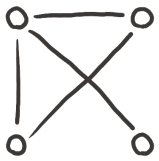
What is the size of the sample space? $|S| = 2^5 = 32$. What is the size of E? There are smarter ways to count it, but we can also just list them in this case (check that $|E| = 16$). So we have

$$P(E) = \sum_{a \in E} P(a) = \frac{16}{32} = \mathbf{\frac{1}{2}}$$

2/27/2025

I substituted for class today, and we talked more about graph connectivity, and vertex & edge cuts. First, we had a refresher on graph basics:

- A graph G is a pair of vertices along with edges between those vertices $G = \langle V, E \rangle$
    - Our graphs are *simple* and *undirected*, e.g.



- The *degree* of a vertex v is its number of neighbors.
- A *walk* is any sequence $v_1 \sim v_2 \sim \ldots v_n$ of vertices (repeats allowed)
- A *path* is a walk with no repeated vertices
- A *circuit* is a path where the start and end vertex are the same, $v_1 = v_n$.
- A graph is *connected* if there is a path from any vertex $u \in V$ to any other vertex $v \in V$.
- A *vertex cut* is a subset $V' \subseteq V$ such that removing it disconnects the graph
- An *edge cut* is a subset $E' \subseteq E$ such that removing it disconnects the graph

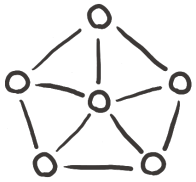
We can measure how connected a graph is (its *connectivity*) by counting how many vertex/edge cuts it takes to disconnect the graph.

Definition. Let G be a graph. Its *vertex connectivity* $\kappa(G)$ is the minimum size of a vertex cut.

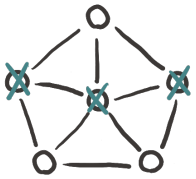
Definition. Let G be a graph. Its *edge connectivity* $\lambda(G)$ is the minimum size of an edge cut.

If the graph represents a network (say a layout of servers), $\kappa(G)$ is the minimum number of servers that can't go down without loss of network-wide service. (Similarly, $\lambda(G)$ is the number of wireless (or wired) connections between these servers that cannot go down.)

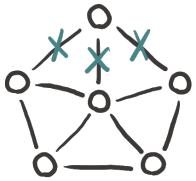
Example. Consider the wheel W_5:



Does it have a vertex cut? Yes, since we can disconnect it like:



Is this the best that we can do? Take a minute to check that any vertex cut of size 2 won't disconnect the graph. And so $\kappa(W_5) = 3$. What about edge cuts? Here's one, just disconnect it as follows:



Is this the best we can do? Again, check that any edge cut of size 2 won't do the job. So $\lambda(W_5) = 3$.

Example. Consider the connected graph K_5:

An edge cut here is easy, just do the following:

Since no edge cut of size 3 will disconnect the graph,we have $\lambda(K_5) = 4$. What about vertex cuts? Well, no matter what subset of vertices we remove, the remaining graph will still connected. This means there *is no* vertex cut for the connected graph.

Notice that there is no vertex cut *or* edge cut for the single-vertex graph. Also, if a graph is already disconnected, it has a trivial vertex/edge cut (the empty set is one for each). We modify the definitions of vertex and edge cut to account for these edge cases.

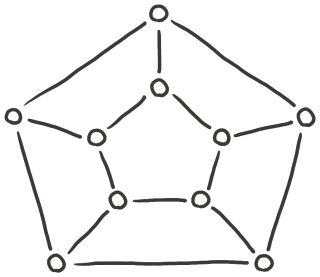
Definition. Let G be a graph. Its *vertex connectivity* $\kappa(G)$ is the minimum size of a vertex cut. If G is:

- a single vertex, $\kappa(G) := 0$

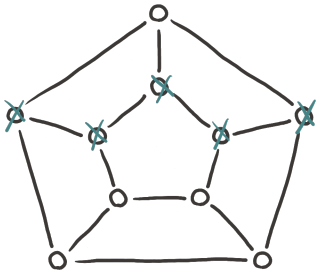
- disconnected, $\kappa(G) := 0$
- a complete graph $G = K_n$, $\kappa(G) := n - 1$ (the maximum possible size)

Definition. Let G be a graph. Its *edge connectivity* $\lambda(G)$ is the minimum size of an edge cut. If G is a single vertex or is disconnected, $\lambda(G) = 0$.

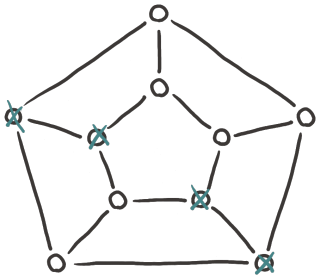
Example. Here's one more example. Consider the graph G:



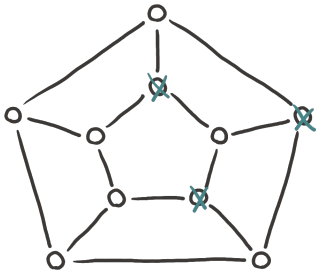
Here's a vertex cut (of size 5):



Is this the best we can do? Not quite—it looks like a cut of size 4 works:

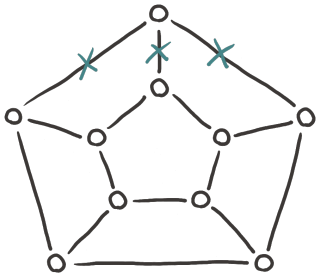


But is *this* the best we can do? Nope! It turns out we have a cut of size 3:



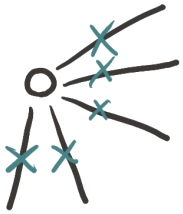
Take a minute to check (carefully) that no cut of size 2 can disconnect the graph. So $\kappa(G) = 3$.

What about edge cuts? Well, we have the following edge cut of size 3:



Check that no cut of size 2 works. So $\lambda(G) = 3$.

Note. What do you notice about edge cuts? What is an easy, guaranteed way to make an edge cut? Looking at the examples above, you can always isolate a single vertex by cutting off all its neighbors—let's say, isolate the vertex with the fewest neighbors.



Theorem. For all graphs $G = \langle V, E \rangle$, $\lambda(G) \leq \min_{v \in V}(\deg(v))$.

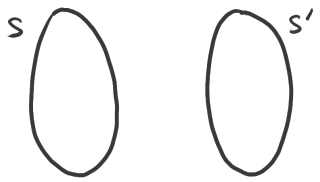
(i.e. the minimum edge cut is at least as small as the minimum degree in the graph)

Proof. We just need to show that there *is* an edge cut of size $\min_{v \in V}(\deg(v))$. (Since $\lambda(G)$ is the smallest edge cut size, it will be at least as small as the edge cut we give.) Let v' be the vertex of smallest degree, i.e. $\deg(v') = \min_{v \in V}(\deg(v))$. Now cut all of the edges of v'. The resulting graph is disconnected, so this constitutes an edge cut of size $\min_{v \in V}(\deg(v))$. □

Note. What do you notice about vertex cuts? In all the examples so far, $\kappa(G) = \lambda(G)$. Can you come up with a graph where they are *not* equal?

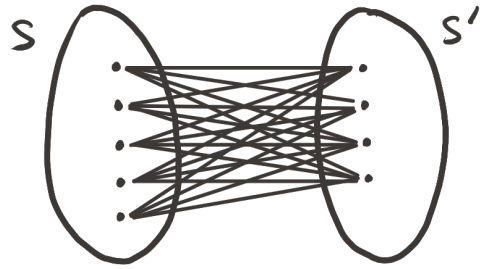
Theorem. For all graphs G, $\kappa(G) \leq \lambda(G)$.

Proof. The proof is a doozy, but it will give you a solid handle on how to think about graphs & their connections in a proof. Let G be a graph with n vertices. First of all, since the maximum number of vertices we can cut is $n-1$, $\kappa(G) \leq n-1$. Now let E' be a minimum edge cut, leaving two parts (not necessarily each connected parts) $S, S' \subseteq G$.



It's easier to first consider the case when S, S' are fully connected (every vertex $u \in S$ is connected to every other vertex $v \in S'$. Then we consider the alternative: There is *some* $u \in S$ that is *not* connected to some vertex $v \in S'$.

Case 1. S, S' are fully connected.



Since E', i.e., a minimum edge cut, separates the graph into these parts, the size of any minimum edge cut must be $|S| \cdot |S'|$ (the number of edges in this fiber connecting the two parts). Moreover, note that $|S| \cdot |S'| \geq n - 1$ (there must be at least as many edges as vertices, since each edge starts at a vertex). Putting this all together, we have

$$\kappa(G) \leq n - 1 \leq \lambda(G)$$

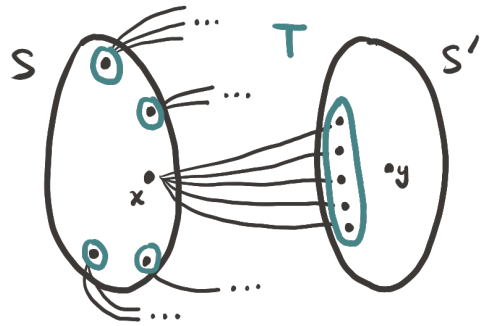
and in this case we're done.

Case 2. S, S' are not fully connected. Let $x \in S$ and $y \in S'$ be the two non-adjacent vertices. Let's now try to give a vertex cut. Any vertex cut would have size $\geq \kappa(G)$, and if we're clever we can find one with size $\leq \lambda(G)$. If we cut x or y, we're doomed—we can't guarantee that S or S' have any other elements in them, so we could not say if that cut actually disconnects the graph.

Try this cut: cut all vertices in S that have ties to S', then cut those vertices in S' that are connected to x. In the first part we ensure that x is the only node in S still connected to S', and in the second part we cut all of its ties to S', so this *does* disconnect the graph. Call this cut T. Here's what we're doing formally:

$$T = \{u \in S - \{x\} \mid \text{there is some } v \in S' \text{ such that } u \sim v\} \cup \{u \in S' \mid x \sim u\}$$

And in a picture:



Since T is a vertex cut, $|T| \geq \kappa(G)$. Now take a minute to see that the edge cut E' we started with must *at least* cut the edges connected to the vertices in T (highlighted in the

picture). So that means $|E'| \geq |T|$. Putting everything together, we have:

$$\lambda(G) = |E'| \geq |T| \geq \kappa(G)$$ □

2/28/2025

We had the exam at the usual time 10:00am after all.