Welcome Back!

P vs NP: Complexity Classes with Graphs

SIGma

Outline

Housekeeping

- Join the Discord!

Section 1

Admins in No Particular Order

Sasha

- Sophomore in CS, double major in physics
- CA for CS 374
- Working on quantum cryptography research
- Participated in error-correcting codes research at USF REU this summer

Alex

- Junior in Stats & CS, double major in Math
- CA for CS 225, previously a CA for CS 128H and CS 374
- Doing compilers adjacent research
- SWE intern at Box this summer

Franklin

- Junior in Math & CS
- CA for CS 374
- SWE internship at CME Group this summer

Ryan

-

Sam

- CS PhD, in TCS, 2nd year
- VR/RE Intern @ Battelle
- SIGma Admin since Fall 2022

Porter

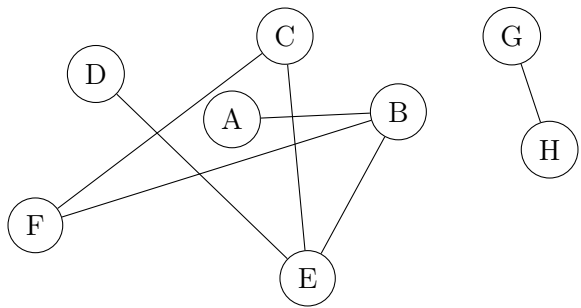
- CS Major; Math Minor; 2 years left in B.S.-M.C.S.
- SWE internship at CDK Global this summer
- CA for CS 128H and CS 225
- Second semester as a SIGma Admin
- Cardio King and Foosball Fanatic

Section 2

Graphs

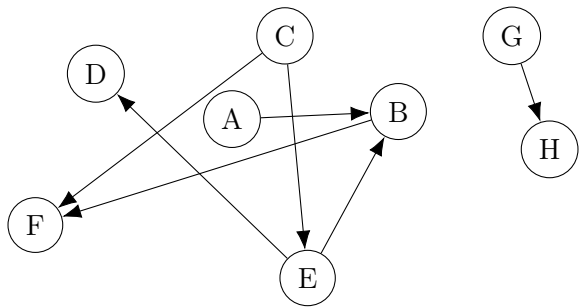
Definitions

- In computer science and abstract math, graphs are a very specific thing.
- A graph, G, consists of a set of vertices, V, and a set of edges, E.
  - $G = (V, E)$



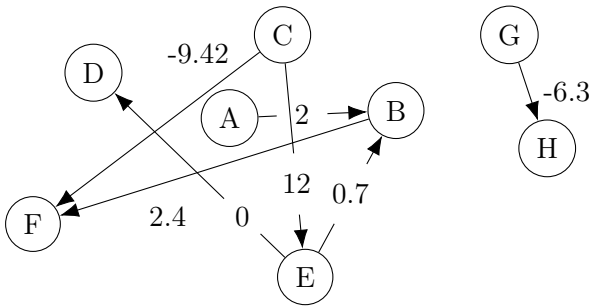
Definitions

Graphs can be directed...



Definitions

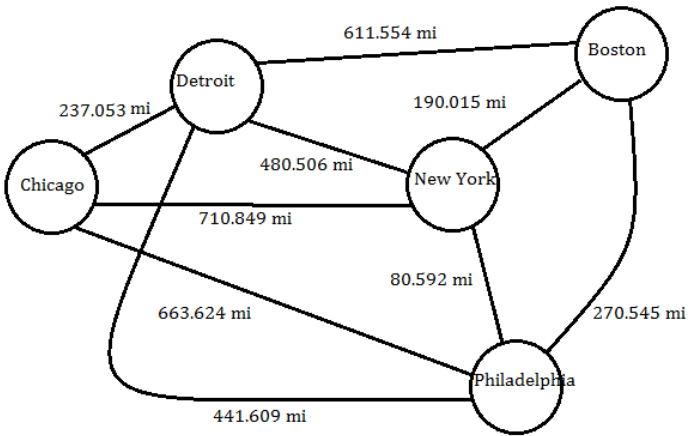
...or weighted.



Definitions Cont.

- If one vertex can be reached by another, they are in the same *connected component*.
- The *degree* of vertex v is the number of edges with v as an endpoint.
- In a *complete* graph, each vertex is connected to all other vertices with an edge.
- *Cycle*: what you get when it's possible to walk in a loop back to the starting vertex.

Maps


611.554 mi
Boston
Detroit
237.053 mi
190.015 mi
480.506 mi
Chicago
New York
710.849 mi
80.592 mi
663.624 mi
270.545 mi
Philadelphia
441.609 mi

Questions?

Section 3

P vs NP

Millennium Prize

- On May 24, 2000, The Clay Mathematics Institute put a $1 million reward on 7 unsolved "Millennium Problems".
  - Only one has been solved, but the winner, Grigori Perelman, turned down the prize due to "disagreement with the organized mathematical community."
- The question of P vs NP is one of the 6 remaining unsolved problems, and proof that $P = NP$ would have major implications in computing and beyond.
  - Cryptography
  - Problem solving

Background

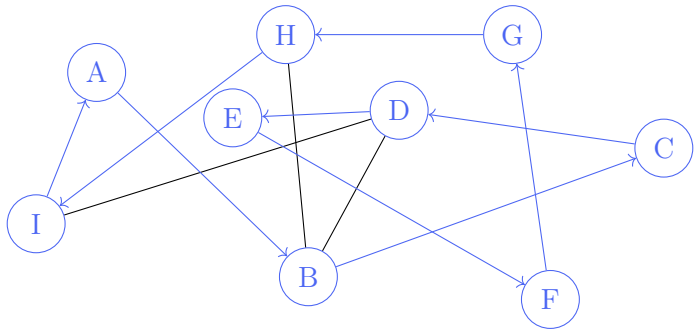
- Big-O analysis is used to analyze the runtime of an algorithm without getting bogged down by relatively insignificant details.
  - If an algorithm is $O(n)$, runtime grows linearly to the size of the input.
  - For $O(n!)$ algorithms, runtime grows factorially to the size of the input.
  - $O(n) = O(\frac{n}{2}) = O(2000 \cdot n + 37) = O(c \cdot n)$
- This type of thinking works because computers operate at scale.
- A *polynomial-time* algorithm has a runtime of the form $O(n^k)$ for some k. Notably, this excludes exponentials and factorials.
- *Deterministic*: a process with a predictable result for a given start state.

P vs NP

- *P*: the set of **decision** problems that a **deterministic** algorithm can solve in polynomial time.
- *NP*: the set of **decision** problems that a **nondeterministic** algorithm can solve in polynomial time. These problems can be **verifed** in polynomial time.
- The big question: "Are these two types of problems truly different?"
- Intuitively (and informally), this asks if problems that can be checked easily can also be solved easily.
  - (Intuitively, it feels like the answer should be no...)

Example: Hamiltonian Cycle

- Given a graph, does a cycle exist that visits each vertex exactly once?



- This is clearly verifiable in polynomial time.
- A brute force algorithm is to try every possible path, which is $O(|V|!)$.

Hamilton's Clairvoyance

- A nondeterministic algorithm is faster: imagine if we could correctly chose the right path at every junction. At that point, are we really solving anything?
- By now, it should seem obvious that $P \neq NP$, but that has **not** been proven...
  - ...so magic algorithms might be possible?!
- This particular problem is *NP-complete*, which means every other problem in NP *reduces* to it.

Questions?

Section 4

Reductions and the Traveling Salesman

But What Are Reductions?

We can show that a problem is in NP if we can use it to solve some other problem that we already know is in NP. This is a proof-by-contradiction of sorts.

Traveling Salesman

Consider a salesman trying to visit some collection of cities on business before returning home. We ask: "Is it possible to visit these cities by traveling $\leq k$ miles?"

Is this problem NP-Hard?

Traveling Salesman Reduction

- Assume we have a polynomial-time algorithm to solve the TSP.
- Now consider an instance of the Hamiltonian Cycle problem with graph $G = (V, E)$.
- We want to use our TSP algorithm to find a Hamiltonian cycle.
- Construct a new weighted graph, $G' = G$ with weights given by $w(u) = 1$ for $u \in V$.
- Now we only have to run the TSP algorithm asking if it is possible to visit all the cities in $\leq |V|$ miles. G has a Hamiltonian Cycle if and only if the algorithm returns "yes."

Traveling Salesman Reduction Cont.

- It took polynomial time to construct G' from G, and our imagined TSP algorithm is also polynomial time, so the whole process took polynomial time.
- But we believe the Hamiltonian Cycle problem is not solvable in polynomial time—a contradiction.
- Thus, our initial assumption that a polynomial-time algorithm to solve the TSP exists is wrong, and the TSP is NP-hard.

Questions?

Current State of P vs NP

- Most experts believe $P \neq NP$, but there is still no proof.
- Many believe that we do not have the mathematical tools for a proof, or even that a proof is impossible in the common axiomatic systems that we have now. [Aar17]

Section 5

Approximate Traveling Salesman

Weekly Brainteaser

After the revolution, each of the 66 citizens of a certain city, including the king, has a salary of 1. King cannot vote, but has the power to suggest changes to the distribution of salaries. Each person's salary must be a **non-negative whole number of dollars**, and the salaries must sum to 66. He suggests a new salary plan for every person including himself in front of the city. Citizens are greedy, and vote yes if their salary is raised, no if decreased, and don't vote otherwise. The majority vote wins. The king proposes a series of plans to maximize his salary. **What is the king's maximum salary?**

Bibliography I

Scott Aaronson.

Is p versus np formally independent.

https://www.scottaaronson.com/papers/indep.pdf, 2017.

Accessed: 09-02-2024.