CS 4102: Algorithms

Lecture 27: Finale

David Wu

Fall 2019

Warm Up

Pick up a slip of paper from the front
Take out a coin

(Pennies up front if you need one)
(Please return at the end of lecture)

Think of embarrassing yes/no questions to ask me

Today's Keywords

Differential privacy (randomized response)

NP completeness

Homework

HW9, **HW10C** due **tonight**, 11pm

- Graphs, Reductions
- Written (LaTeX)
- No late submissions for HW10C

Final Exam

Monday, December 9, 7pm in Olsson 120

- Practice exam out
- Review session on Saturday 1pm (email with location coming soon)
- SDAC: Please sign-up for a time on December 9

Academic Integrity

SECTIONS HOME SEARCH

President Trump Expected to Shrink Bears Ears by as Much as 90 Percent

Ministers Look to Revive Martin Luther King's 1968 Poverty Campaign

As Computer Codi

By JESS BIDGOOD and JEREMY B. MERRILL MAY

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS SIGN IN

BIZ & IT —

Code copypasta increasingly common in CS education

Roughly 22 percent of Stanford honor code violations involve plagiarism in ...

RYAN PAUL - 2/12/2010, 5:11 PM

THE DAILY ILLINI

The independent student newspaper at the University of Illinois

NEWS SPORTS OPINIONS LIFE & CULTURE SPECIAL SECTIONS LONGFORM BUZZ CLASSIFIEDS

College of Engineering piloting program to combat cheating

Top Stories

Thoughts?

Our Collaboration Policy

You are encouraged to collaborate with up to 4 other students, but all work submitted must be your own *independently* written solution. Do not seek published or online solutions for any assignments. If you use any published or online resources (which may not include solutions) when completing this assignment, be sure to cite them. Do not submit a solution that you are unable to explain orally to a member of the course staff. Please remember that you are not allowed to share any written notes or documents (these include but are not limited to Overleaf documents, LaTeX source code, homework PDFs, group discussion notes, etc.). Any solutions that share similar text/code will be considered in breach of this policy.

Thoughts?

Differential Privacy

Statistical mechanism to measure sensitive attributes about a population without compromising individual privacy

- **Example:** Are you now or have you ever been a member of the Communist Party of the United States?

Enables accurate measurement at the population level, but not the individual level

Privacy requirement: whether an individual participates or not in the study has very little (negligible) effect on the outcome of the study

Randomized Response

Very old technique (1965), now used by Google for collecting/analyzing user data (Rappor)

Flip a fair coin:

- If heads, respond "yes"
- If tails, answer the question truthfully

In this case, a "no" answer only arises if the individual answers truthfully

Can also consider a variant with three options: "answer yes," "answer no," and "answer truthfully"

Privacy: Suppose you answer "yes" to a sensitive question

- With probability 50%, answer is "yes" because the coin landed heads
- More likely that a "yes" answer is due to coin landing heads than attribute being true

Questions!

Randomized Response

On the final exam (for extra credit):

As far as you're aware, did you, at any point this semester, violate the collaboration policy in CS 4102?

Randomized Response

Assume everyone participates honestly

We know 50% of “yes” answers were from the coin landing **heads**

- If 100 people participate, eliminate 50 “yes” responses
- Proportion of “yes” answers given by remaining “yes” answers

Consider a person who answers “no”

- We know this person didn’t cheat

Consider a person who answers “yes”

- Most people ($\geq 50\%$) who answered “yes” only did so because the coin landed **heads**
- It is still **more** likely that this person **did not cheat**

Randomized Response

Your Turn!

Flip a coin:

- If heads, respond “yes”
- If tails, truthfully answer an embarrassing question:
  - **Have you ever streaked the lawn?**
    - Write “yes” or “no”
    - Pass the slip to your left

At the end, tally total “yes” and total “no” and pass totals forward

What is the Nature of the World?

Impagliazzo's Five Worlds

Describes what computer science might look like depending on how certain open questions are answered

Algorithmica

Heuristica

Pessiland

Minicrypt

Cryptomania

The Story: Gauss vs. Büttner

Büttner's goal: embarrass Gauss

Come up with a problem which Gauss finds difficult but Büttner can solve quickly

1. Come up with a graph and a vertex cover
2. Give the graph to Gauss
3. When Gauss is stumped, show the vertex cover

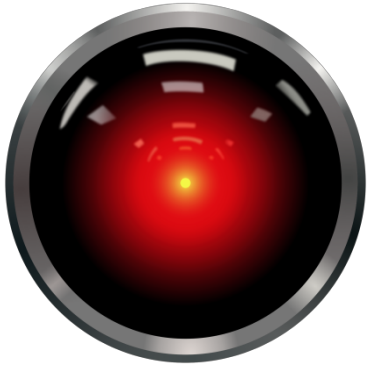
Algorithmica

$\boldsymbol{P = NP}$

NP problems solvable in polynomial time

Gauss can quickly find the solution to Büttner's problem

Gauss is not embarrassed



Advantages:

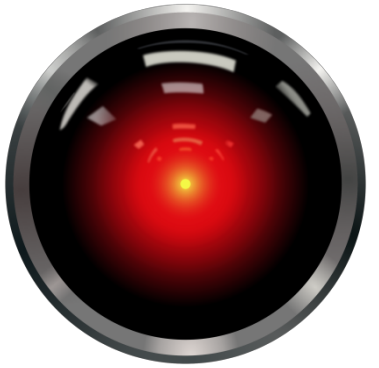
- VLSI Design
- Strong AI
- Cure for cancer?

Disadvantages:

- No privacy
- Computers take over

Algorithmica

$\boldsymbol{P = NP}$



NP problems solvable in polynomial time

Gauss can quickly find the

Gauss is not embarrassed

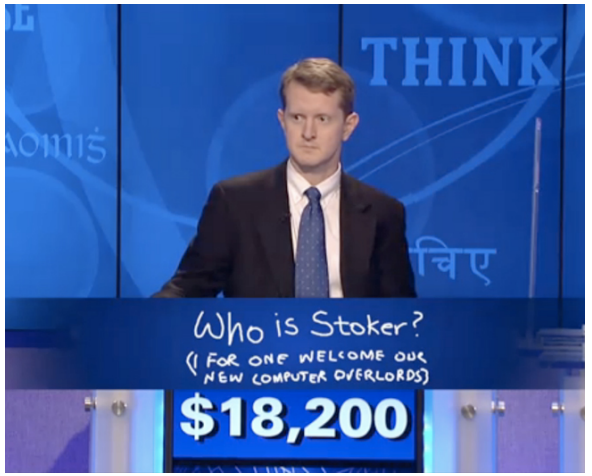
Note: polynomial time does not necessarily mean concretely efficient (e.g., $O(n^{1000})$ may not be very practical)

Advantages:

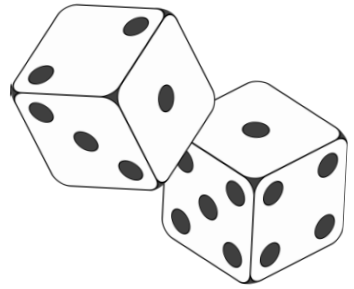
- VLSI Design
- Strong AI
- Cure for cancer?

Disadvantages:

- No privacy
- Computers take over



Heuristica



$P \neq NP$ in the worst case, but problems are easy on average

Time to come up with a problem ≈ time to solve it

Büttner can give hard problems, but it is hard to find them (as hard as it is to solve them)

Gauss is not embarrassed

Advantages:

- Similar to Algorithmica
- Depends on real-world distributions

Disadvantages:

- Bad real world distributions could make things hard to solve
- No privacy

Pessiland

$P \neq NP$, there exist problems that are hard on average, but one-way functions do not exist

Hard problems are abundant, but cannot easily find a hard problems together with its solution

Gauss can be stumped, but Büttner will also not know the answer

Advantages:

- Universal compression
- Reverse engineering

Disadvantages:

- No privacy
- No algorithmic advantages
- Progress is slow

Minicrypt

$P \neq NP$, one-way functions exist, no public key cryptography

Büttner can give hard problems to Gauss and also know their solutions

Gauss is embarrassed

Advantages:

- Symmetric cryptography
- Authentication
- Derandomization

Disadvantages:

- No key-agreement

Cryptomania

$P \neq NP$, public-key encryption exists

Büttner can come up with problems and solutions, and publicly share the solution with all other students except Gauss

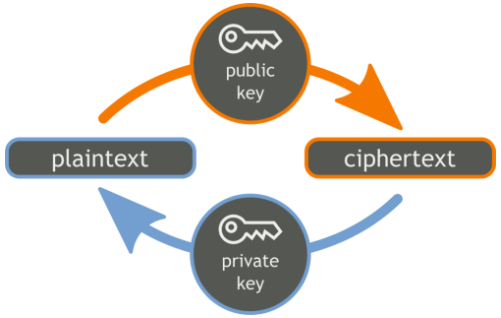
Gauss is very embarrassed

Advantages:

- Cryptography

Disadvantages:

- Algorithmic progress will be slow



What's Next?

Does $P = NP$?

Can we solve 3*-SAT in linear time?*

Beyond P *vs.* NP*:* PH, PSPACE, EXP

Computational Complexity

CS 4102

What's Next?

Computational Complexity

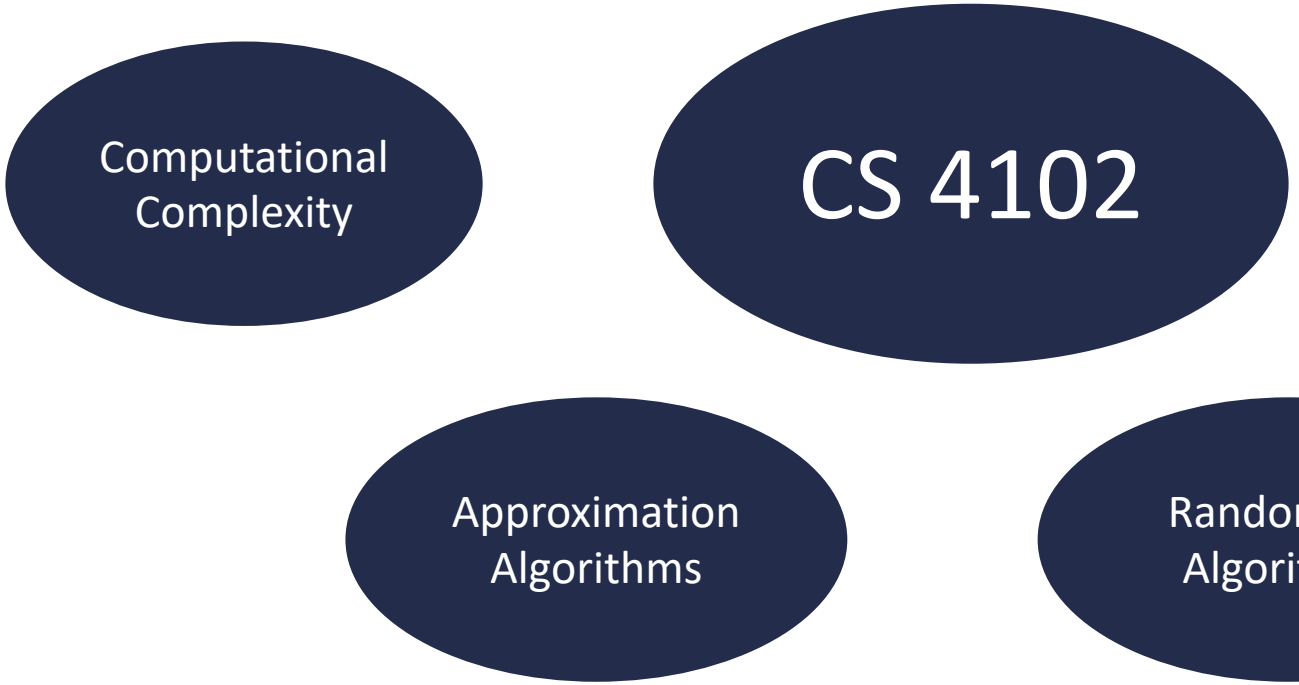
CS 4102

Approximation Algorithms

Given a graph, can we find a vertex cover that is close to optimal?

Can we approximate sequence alignment (e.g., longest common subsequence) in linear time?

What's Next?

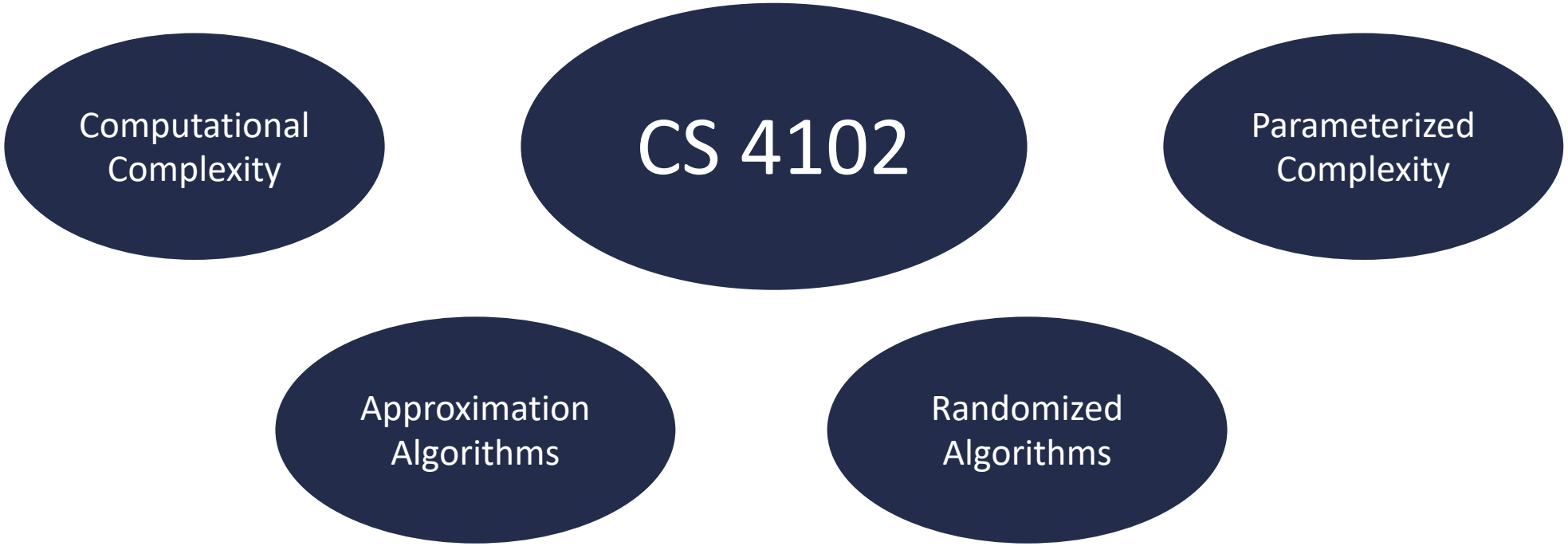


Min-cut: *<u>randomized</u>* $O(|E|)$ *algorithm*

Closest pair of points: *<u>randomized</u>* $O(n)$ *algorithm*

What's Next?

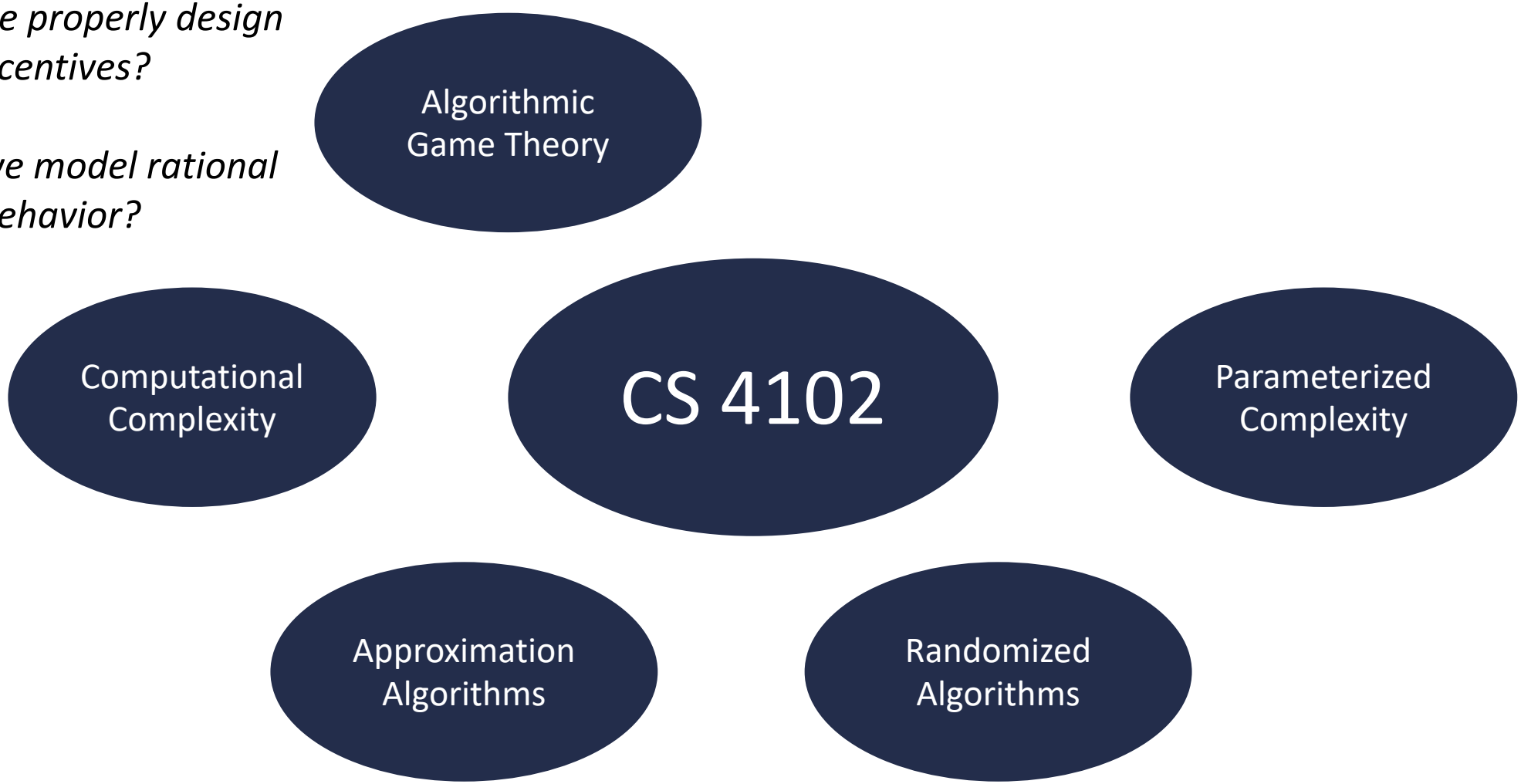
On what types of graphs is it easy to compute vertex covers?



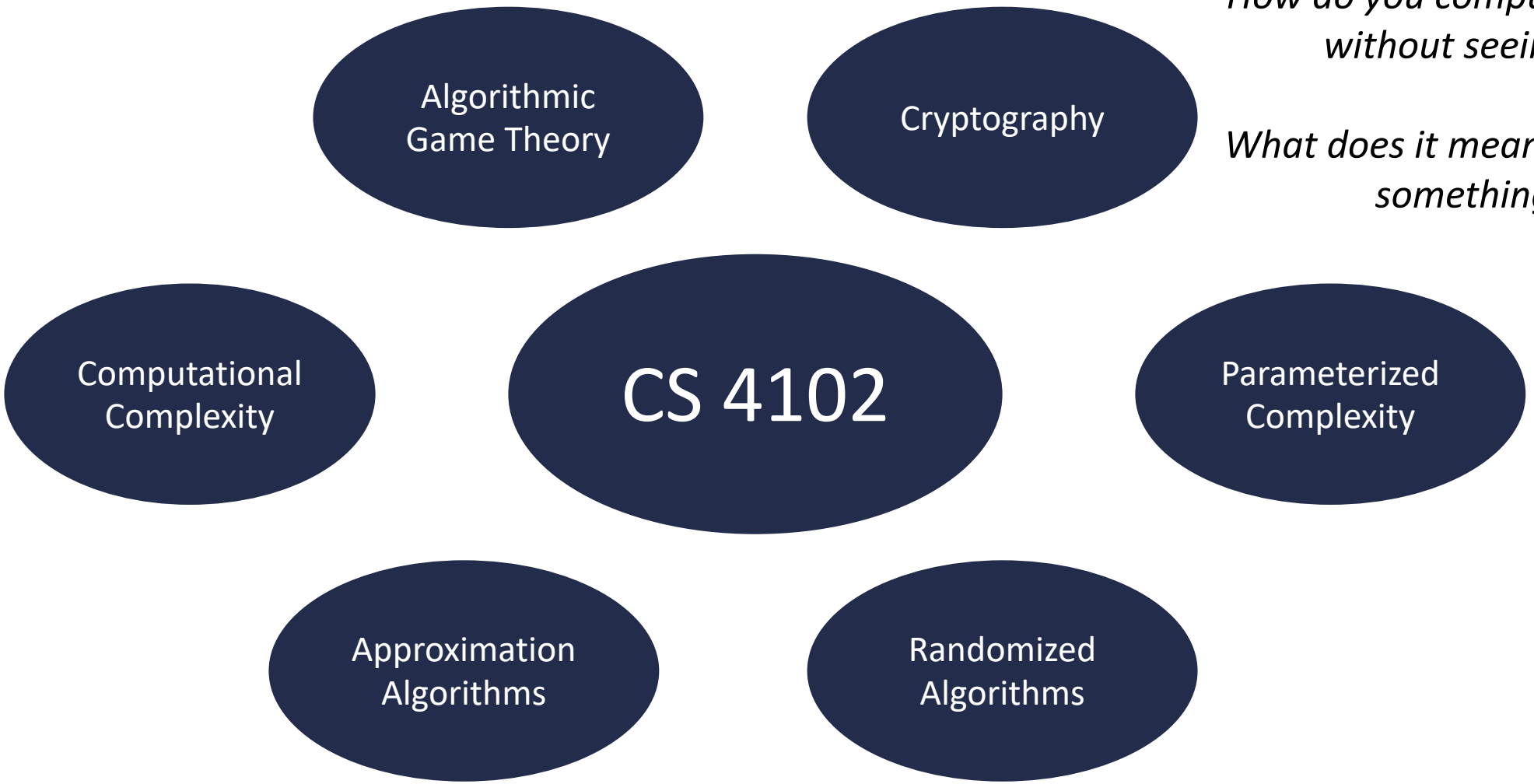
What's Next?

How do we properly design incentives?

How do we model rational behavior?



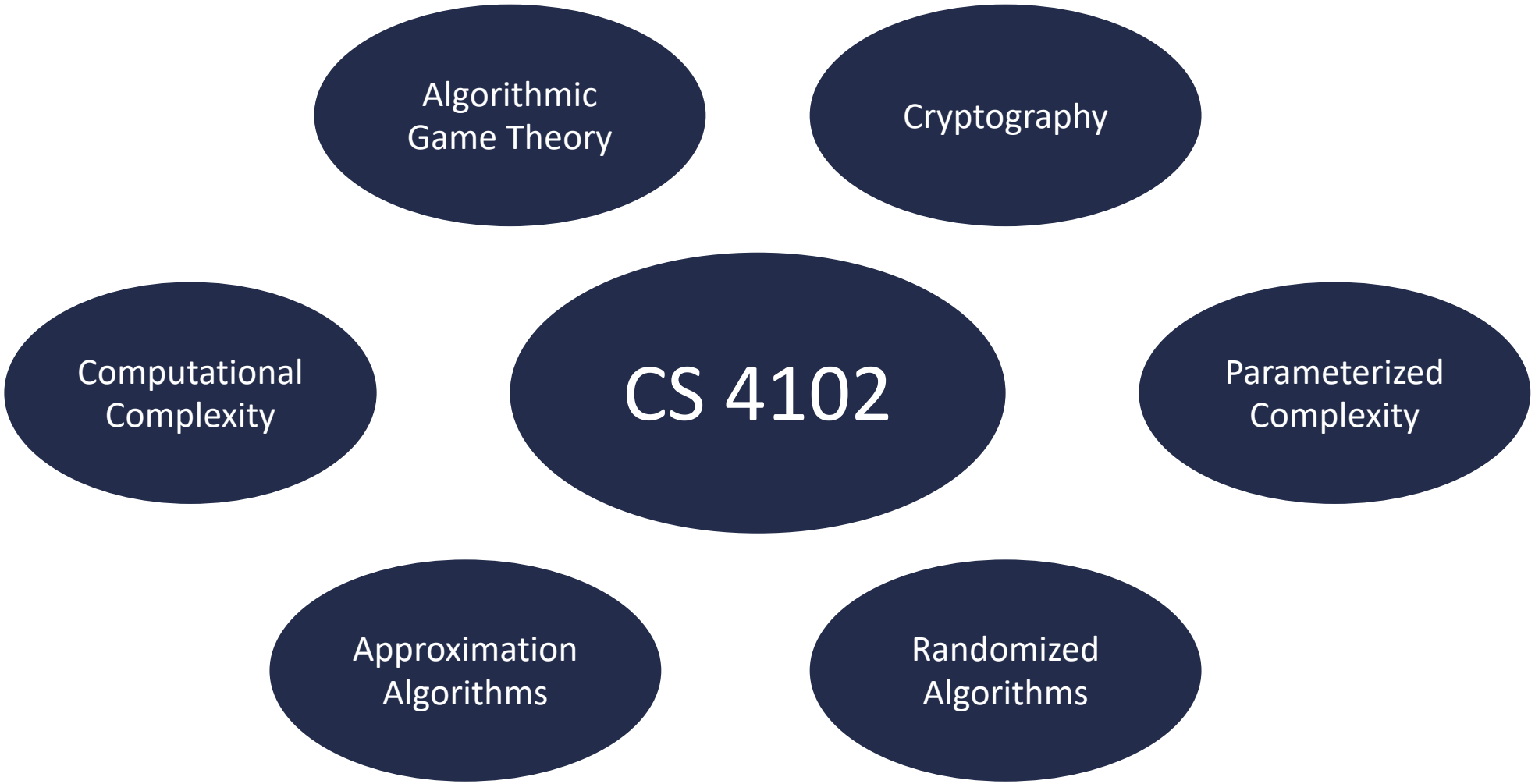
What's Next?



How do you compute on data without seeing it?

What does it mean to "know" something?

The End


Algorithmic Game Theory
Cryptography
Computational Complexity
CS 4102
Parameterized Complexity
Approximation Algorithms
Randomized Algorithms