CS265/CME309, Fall 2020

Class 1: Agenda, Questions, and Links

1 Welcome!

Welcome to CS265/CME309!

1.1 Introductions

- Course staff introductions.
- Poll: http://PollEv.com/cs265.

1.2 Course Logistics

- (presentation with some slides)

2 Polynomial Identity Testing

2.1 Group work

- Find a room in the Nooks community; aim for $3-6$ people per room.
- Feel free to make a new room if you (and your colleagues) want a custom name!
- If you're not in a position to interact right now, go to the "Quiet Room" and work on these problems on your own.
- If you have questions during group work:
  - Ask in chat (either to everyone or directly to the course staff).
  - Come to the "Teaching Team" room and ask us.
  - Say in the chat that you have a question, and one of us will stop by.

Group Work

Important: as you make progress on the question(s), one person in each room should record your progress on http://PollEv.com/cs265.

(**10-20 minutes**, depending on how fast folks go through these)

1. First, introduce yourselves to each other. What year/program are you in? What

class/activity/etc are you most excited about for this quarter?

2. Quietly read the following definition.

   > A polynomial $f(x)$ is *identically zero* if all its coefficients are zero. For example, the polynomial $f(x) = (x-1)(x+1) + 1 - x^2$ is identically zero because when you expand it out, all of the terms cancel.

3. Discuss: are there any questions about the definition? (If there are questions that the group can't resolve, ask in chat or pop over to the "Teaching Team" room to ask in person!)

4. Which of the following two polynomials are identically zero?

$$f(x) = (x+1)^2(x-2)^2 + x^2(3+2x-x^2) - 4(x+1)$$

$$g(x) = (2x+1)^2(x-3)^2 - x^2(1+x+2x^2) - (5x+9)$$

   Once you have answered this, fill out the corresponding polleverywhere.

5. Suppose I were to give you a polynomial $f(x)$ of total degree n and ask you if it is identically zero or not. How long, asymptotically, would it take you in the worst case if you were to do this in the straightforward way, by expanding out every term?

   (a) $O(n)$

   (b) polynomial in n

   (c) $2^{\Omega(n)}$

   Hint: Think about $f(x) = \prod_{i=1}^{n}(x + a_i)$ for some numbers a_i. How long would it take you to compute the coefficient on, say, $x^{n/2}$?

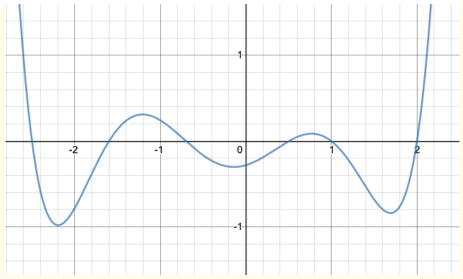
   Once you have answered this, fill out the corresponding polleverywhere.

6. At the end of this group work, I am going to challenge you with degree-8 polynomials f and g, and ask you which is identically zero. You're going to have **one minute** to answer. Think now about an efficient way to answer this challenge.

   As part of your strategy, you may use a basic calculator (eg, https://www.google.com/search?q=calculator), but dumping the expression into WolframAlpha for it to plot or simplify (or something like that) is cheating.

   Hint: Remember that this is a class on randomized algorithms. Can you think of a randomized strategy?

   Hint: Here is the graph of a polynomial that is *not* identically zero. What is true about the values $g(x)$ for most choices of x?



Once you think you have a strategy, fill out the corresponding pollev-erywhere.

7. Would your strategy still work if I know it ahead of time? That is, if I know the strategy, but not necessarily the outcome of any randomness in the strategy, could I come up with polynomials f, g that would foil your strategy?

   If your strategy would fail if I know it ahead of time, try to come up with another strategy that would succeed!

8. Can you adapt your strategy to work for multivariable polynomials? (eg, polynomials $f(x, y, z)$?)

Group Work: Solutions

4. $f(x)$ is identically zero, and $g(x)$ is not.

5. Naively, this takes time $2^{\Omega(n)}$. In the example in the hint, suppose that $f(x) = \prod_{i=1}^{n}(x + a_i)$. Then the coefficient on $x^{n/2}$ is

$$\sum_{S \subseteq [n], |S| = n/2} \prod_{i \in S} a_i.$$

   There are $\binom{n}{n/2}$ things in this sum, which is at least $2^{\Omega(n)}$.

   Several people during class pointed out that there are faster ways than this naive compute-all-of-the-coefficients-by-expanding-everything-out approach! In fact there are! For the multivariate case, though, it gets a bit trickier. What would you do for an n-variate polynomial?

6. There are lots of strategies that would work! Some good ideas include:

   - Plug in 10000 and see if you get zero. Since nonzero polynomials go to $\pm\infty$ as $x \to \infty$, and since Mary surely wouldn't choose a polynomial with super tiny coefficients, $f(10000)$ will probably be non-zero if f is.

- Compute just the constant term, or the coefficient on x^n. Both of those are pretty easy to compute just by looking at the function. If they're not zero, then say the polynomial is not zero.
- Choose a random evaluation point Z in the set $\{1, 2, \ldots, 1000\}$. If $f(Z)$ is not zero, then certainly f is not identically zero. Since this polynomial is going to have at most 8 roots, the probability that $f(Z) = 0$ if f is nonzero is at most $8/1000$, which is pretty small.

All of these are good ideas (and there are more good ideas!) However, the first two are not robust if I know them ahead of time—I could cook up some "bad" examples for them. The last one is robust!

2.2 Challenge and Discussion!

- Go to http://PollEv.com/cs265 and get ready for your challenge!
- After that's done, refresh http://PollEv.com/cs265 and describe your solution. If you see another group's solution that is similar to yours (or if you just like it), upvote it!
- (Short presentation on Polynomial Identity Testing, with slides)

3 What is a randomized algorithm?

- (Presentation with slides)
- Go to http://PollEv.com/cs265: how would you boost the success probability for a one-sided algorithm?
- (Presentation with slides)
- Another PollEv: how would you boost the success probability for a two-sided algorithm?

4 Wrap Up

Before next time:

- Watch the two short videos for Class 2 on Canvas.
- Do the associated short quiz.