Class 1: Agenda and in-class Questions

1 Welcome!

Welcome to CS265/CME309!

1.1 Introductions and Course Logistics

- All logistics info can be found on http://web.stanford.edu/class/cs265

2 Polynomial Identity Testing

2.1 Group work

Group Work

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. Read the following definition.

   A multivariate polynomial $f(x_1, \ldots, x_m)$ is *identically zero* if all its coefficients are zero. For example, the polynomial $f(x_1, x_2) = (x_1 + 1)(x_2 + 1) - 1 - x_1 x_2 - (x_1 + x_2)$ is identically zero because when you expand it out, all of the terms cancel.

   Now, work on the following questions with your group.

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

   $$f(x, y) = (x - y)^2 + 2xy + (x + y)^3 - y(3x^2 + y(3x + y + 1)) - (x + 1)x^2$$

 $$g(x, y) = (x - 2y)^2 + xy + (x + y)^3 - y(3x^2 + y(3x + y + 1)) - (x + 1)x^2$$

4. Let $f(x_1, x_2, \ldots, x_n)$ be a polynomial in n variables of total degree[a] at most n. Suppose that you are given an expression for f that has length $O(n)$. How long, asymptotically, would it take you to decide if f were identically zero 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) $2^{\Omega(n)}$

5. At the end of this group work, we are going to challenge you with two 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: *You might take inspiration from the univariate case. Here's the graph of a polynomial $g(x)$ that is* not *identically zero. What is true about the values $g(x)$ for most choices of x?*
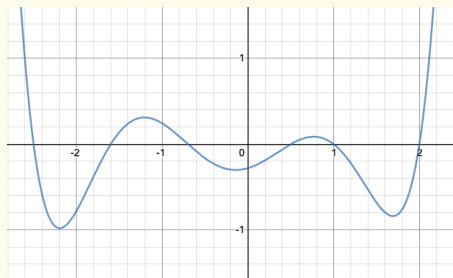
6. Would your strategy still work if Mary knew it ahead of time? That is, if I know your strategy — but not necessarily the outcome of any randomness in the strategy — could I come up with polynomials f, g that would foil your strategy?

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

7. If you've finished all of the above, try to come up with an efficient *deterministic* strategy that would succeed at this task.

---

[a]the *total degree* of a monomial $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ is $\sum_{i=1}^{n} a_i$. The total degree of a polynomial is the largest total degree of any monomial that appears in it.

Group Work: Solutions

3. f is identically zero, and g is not.

4. Naively, this takes time $2^{\Omega(n)}$. That's because there are $\binom{2n}{n} = 2^{\Omega(n)}$ possible monomials of degree n, so I need to compute at least that many coefficients to check.

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

   - Plug in 10000 (or some other big number) for all of the variables and see if you get zero. Since nonzero polynomials go to $\pm\infty$ as the inputs $x_i \to \infty$, and

since Mary surely wouldn't choose a polynomial with super tiny coefficients, $f(10000, 10000, 10000, \ldots, 10000)$ will probably be non-zero if f is.

- Compute just the constant term, or the coefficient on x_1^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. Again, if Mary doesn't know that you are going to be looking at the constant term (or whatever) if they choose a non-zero polynomial it probably won't have a zero constant term.

- Choose a random evaluation point $(Z_1, Z_2, \ldots, Z_8)$ (say, according to a Gaussian). If $f(Z_1, \ldots, Z_8)$ is not zero, say that f is not identically zero. Otherwise, guess that f is identically zero.

  How likely is this to be correct? If f is identically zero, we will always be correct. If f is *not* identically zero, then we claim that we'll find a nonzero value of it with probability 1. Intuitively, the set of zeros of any degree-8 polynomial is a very small set—it has measure zero in $\mathbb{R}^8$—so no matter what nonzero polynomial is chosen, we will almost always hit a nonzero value.

  Notice that we can't *actually* choose a random real number to test our polynomial at — it would take an infinite amount of time to write that number down. Instead, we would *discretize*, and, say, choose a random element from some finite set that's fixed ahead of time. It turns out that this still works quite well, as we will see in the next part of the agenda!

6. All of the above 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!

7. This is actually an open question! (Sorry :))

2.2   Challenge and Discussion!

- Challenge time!

- A bit of lecture on Polynomial Identity Testing and the Schwartz-Zippel Lemma (see Lecture notes for recap or if you couldn't make it to class).

3   What is a randomized algorithm?

- A bit of lecture about the basic framework for randomized algorithms, if time. (In case we don't get to this or if you couldn't make it to class, there's also a YouTube video you can watch later – link on course website – and it's in the lecture notes).

4   Wrap Up

Before next time:

- Watch the two short videos for Class 2 on YouTube (link on course website).

- Do the quiz on Gradescope.