CS 70 Discrete Mathematics and Probability Theory
Spring 2019 Course Notes

DIS 5A

1 Roots

Recall that a polynomial of degree d has at most d roots. In this problem, assume we are working with polynomials over $\mathbb{R}$.

(a) Suppose $p(x)$ and $q(x)$ are two different nonzero polynomials with degrees d_1 and d_2 respectively. What can you say about the number of solutions of $p(x) = q(x)$, in terms of d_1 and d_2? How about $p(x) \cdot q(x) = 0$?

(b) Consider the degree 2 polynomial $f(x) = x^2 + ax + b$. Show that if f has exactly one root, then $a^2 = 4b$.

(c) What is the *minimum* number of real roots that a nonzero polynomial of degree d can have? How does the answer depend on d?

Solution:

(a) A solution of $p(x) = q(x)$ is a root of the polynomial $p(x) - q(x)$, which has degree at most $\max(d_1, d_2)$. Therefore, the number of solutions is also at most $\max(d_1, d_2)$.

A solution of $p(x) \cdot q(x) = 0$ is a root of the polynomial $p(x) \cdot q(x)$, which has degree $d_1 + d_2$. Therefore, the number of solutions is at most $d_1 + d_2$.

(b) If there is a root c, then the polynomial is divisible by $x - c$. Therefore it can be written as $f(x) = (x-c)g(x)$. But $g(x)$ is a degree one polynomial and by looking at coefficients it is obvious that its leading coefficient is 1. Therefore $g(x) = x - d$ for some d. But then d is also a root, which means that $d = c$. So $f(x) = (x-c)^2$ which means that $a = -2c$ and $b = c^2$, so $a^2 = 4b$.

(c) If d is even, the polynomial can have 0 roots (e.g., consider $x^d + 1$, which is always positive for all $x \in \mathbb{R}$). If d is odd, the polynomial must have at least 1 root (a polynomial of odd degree takes on arbitrarily large positive and negative values, and thus must pass through 0 inbetween them at least once).

2 Interpolate!

Find the lowest-degree polynomial $P(x)$ that passes through the points $(1,4), (2,3), (5,0)$ modulo 7.

Solution:

First, observe that we don't need to compute $\Delta_5(x)$, since it will be multiplied by 0 anyway.

$$\Delta_1(x) \equiv \frac{(x-2)(x-5)}{(1-2)(1-5)} \equiv \frac{x^2-7x+10}{4} \equiv 2\cdot(x^2+3) \equiv 2x^2+6 \pmod 7$$

$$\Delta_2(x) \equiv \frac{(x-1)(x-5)}{(2-1)(2-5)} \equiv \frac{x^2-6x+5}{-3} \equiv 2\cdot(x^2-6x+5) \equiv 2x^2+2x+3 \pmod 7$$

$$P(x) \equiv y_1\Delta_1(x)+y_2\Delta_2(x) \equiv 4\cdot(2x^2+6)+3\cdot(2x^2+2x+3) \equiv 14x^2+6x+33$$

$$\equiv \boxed{6x+5} \pmod 7.$$

Alternatively, you can graph the points in GF(7) and observe that they all lie on $y=-x+5$, which is equivalent to $\boxed{6x+5}$ modulo 7.

3 Secrets in the United Nations

The United Nations (for the purposes of this question) consists of n countries, each having k representatives. A vault in the United Nations can be opened with a secret combination $s \in \mathbb{Z}$. The vault should only be opened in one of two situations. First, it can be opened if all n countries in the UN help. Second, it can be opened if at least m countries get together with the Secretary General of the UN.

(a) Propose a scheme that gives private information to the Secretary General and n countries so that s can only be recovered under either one of the two specified conditions.

(b) The General Assembly of the UN decides to add an extra level of security: in order for a country to help, all of the country's k representatives must agree. Propose a scheme that adds this new feature. The scheme should give private information to the Secretary General and to each representative of each country.

Solution:

(a) Create a polynomial of degree $n-1$ and give each country one point. Give the Secretary General $n-m$ points, so that if he collaborates with m countries, they will have $n-m+m=n$ points and can reconstruct the polynomial. Without the General, n countries can come together and also recover the polynomial. No combination of the General with fewer than m countries can recover the polynomial.

Alternatively, we can have two schemes, one for each condition. For the first condition: just one polynomial of degree $\leq n-1$ would do, where each country gets one point. The polynomial evaluated at 0 would give the secret. For the second condition: one polynomial is created of degree $m-1$ and a point is given to each country. Another polynomial of degree 1 is created, where one point is given to the secretary general and the second point can be constructed from the first polynomial if m or more of the countries come together. With these two points, we have a unique 1-degree polynomial, which could give the secret evaluated at 0.

(b) The scheme in part (a) remains the same, but instead of directly giving each country a point on the $n-1$ degree polynomial to open the vault, construct an additional polynomial for each country that will produce that point.

Each country's polynomial has degree $k-1$, and a point is given to each of the k representatives of the country. Thus, when they all get together they can produce a point for either of the schemes.