CS 70 Discrete Mathematics and Probability Theory Spring 2019 Satish Rao and Babak Ayazifar 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*?

2 Interpolate!

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