CS 70 Discrete Mathematics and Probability Theory
Fall 2016 Seshia and Walrand

Discussion 6A

1. **How many polynomials?**

   Let $P(x)$ be a polynomial of degree 2 over GF(5). As we saw in lecture, we need $d+1$ distinct points to determine a unique d-degree polynomial.

   (a) Assume that we know $P(0) = 1$, and $P(1) = 2$. Now we consider $P(2)$. How many values can $P(2)$ have? How many distinct polynomials are there?

   (b) Now assume that we only know $P(0) = 1$. We consider $P(1)$, and $P(2)$. How many different $(P(1), P(2))$ pairs are there? How many different polynomials are there?

   (c) How many different polynomials of degree d over $GF(p)$ are there if we only know k values, where $k \leq d$?

2. **Lagrange Interpolation**

   Find a unique real polynomial $p(x)$ of degree at most 3 that passes through points $(-1,3)$, $(0,1)$, $(1,2)$, and $(2,0)$ using Lagrange interpolation.

   (a) Find $\Delta_{-1}(x)$ where $\Delta_{-1}(0) = \Delta_{-1}(1) = \Delta_{-1}(2) = 0$ and $\Delta_{-1}(-1) = 1$.

   (b) Find $\Delta_0(x)$ where $\Delta_0(-1) = \Delta_0(1) = \Delta_0(2) = 0$ and $\Delta_0(0) = 1$.

   (c) Find $\Delta_1(x)$ where $\Delta_1(-1) = \Delta_1(0) = \Delta_1(2) = 0$ and $\Delta_1(1) = 1$.

   (d) Find $\Delta_2(x)$ where $\Delta_2(-1) = \Delta_2(0) = \Delta_2(1) = 0$ and $\Delta_2(2) = 1$.

   (e) Reconstruct $p(x)$ by using a linear combination of $\Delta_{-1}(x)$, $\Delta_0(x)$, $\Delta_1(x)$ and $\Delta_2(x)$.

3. **Secret Sharing**

   Suppose the Oral Exam questions are created by 2 TAs and 3 Readers. The answers are all encrypted, and we know that:

   - Both TAs should be able to access the answers
   - All 3 Readers can also access the answers
   - One TA and one Reader should also be able to do the same

   Design a Secret Sharing scheme to make this work.

4. **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. 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.

5. **Sanity check!**

(a) Alice wants to send a message of length 10 to Bob over a lossy channel. What is the degree of the unique polynomial she should use to encode her message?

(b) Alice sent Bob the values of the above polynomial at 16 distinct points. How many erasure errors can Bob recover from?

(c) How many general errors can Bob recover from?