EECS 70 Discrete Mathematics and Probability Theory
Fall 2015 Satish Rao

Discussion 7A

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.

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

2. 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?

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

2. Erasures: Lagrange or Linear System

Say we do the erasure coding scheme discussed in note 10, where a three packet message is sent using a polynomial $P(x)$, where $P(0) = m_1, P(1) = m_2$, and $P(2) = m_3$, and $P(3)$ and $P(4)$ are also sent. The channel loses $P(0)$ and $P(4)$.

In this exercise, we will try to find the polynomial $P(x)$ of degree at most 2 with coefficients in GF(5) such that $P(1) = 2 \pmod 5$, $P(2) = 4 \pmod 5$, and $P(3) = 3 \pmod 5$ and recover the original message.

1. Find the $\Delta_i(x)$ polynomials for $i \in \{1,2,3\}$.

2. Combine the Δ_is with the right coefficients to find the polynomial $P(x)$.

3. Now we will try a different approach. Write the polynomial $P(x)$ as $c_0 + c_1 x + c_2 x^2$. Treating c_is as variables, what do the equations $P(1) = 2 \pmod 5$, $P(2) = 4 \pmod 5$, and $P(3) = 3 \pmod 5$ tell us about the c_is?

4. Solve the system of equations you got from the last part to solve for the c_is. What is the resulting polynomial $P(x)$?

5. What was the original message that was sent?

3. Berlekamp-Welch for general errors

Suppose you want to send your friend a length $n = 3$ message, m_0, m_1, m_2, with advice on a cool place to visit. Unfortunately your only way to communicate with her is via a channel with the possibility for $k = 1$ error. We will work mod 13, so we can encode 13 letters as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

You encode the message by finding the degree ≤ 2 polynomial $P(x)$ that passes through $(0, m_0)$, $(1, m_1)$, and $(2, m_2)$, and then send your friend the five packets $P(0), P(1), P(2), P(3), P(4)$ over the noisy channel. The message your friend receives is

$$\text{CELJH} \Rightarrow 2, 4, 11, 9, 7 = r_0, r_1, r_2, r_3, r_4$$

which could have up to 1 error.

1. First locate the error, using an error-locating polynomial $E(x)$. Let $Q(x) = P(x)E(x)$. Recall that

$$Q(i) = P(i)E(i) = r_i E(i), \quad \text{for} \quad 0 \leq i < n + 2k$$

What is the degree of $E(x)$? What is the degree of $Q(x)$? Using the relation above, write out the form of $E(x)$ and $Q(x)$, and then a system of equations to find both these polynomials.

2. Ask your GSI for $Q(x)$. What is $E(x)$? Where is the error located?

3. Finally, what is $P(x)$? Use $P(x)$ to determine the original (and awesome) message that you sent your friend.