CS 70 Discrete Mathematics and Probability Theory
Fall 2016 Seshia and Walrand **Discussion 6B**

1. **Polynomial Intersections**

   Polynomial intersections Find (and prove) an upper-bound on the number of times two distinct degree d polynomials can intersect. What if the polynomials' degrees differ?

   Solution: They can intersect up to d times. This is because we can specify d points to be the same for both polynomials, then the (d +1)th point to be different. Then the polynomials will be distinct, but still agree at d points. If d+1 points agree, the polynomials will be identical. If the polynomials have degrees d_1 and d_2, with $d_1 > d_2$, then they can intersect up to d_1 times. Pick d_1 points on the polynomial of degree d_2, and another point not on this polynomial. Then a unique degree d_1 polynomial will go through these $d_1 + 1$ points.

2. **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?

   Solution: 5 polynomials, each for different values of $P(2)$.

   (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? **Solution:** Now there are 5^2 different polynomials.

   (c) How many different polynomials of degree d over $GF(p)$ are there if we only know k values, where $k \leq d$? **Solution:** p^{d+1-k} different polynomials. For $k = d+1$, there should only be 1 polynomial.

3. **Remainder Riddles**

   There exists a polynomial (over $GF(7)$) $p(x)$ that has a remainder of 3 when divided by $x-1$, a remainder of 1 when divided by $x+1$, and a remainder of $2x+1$ when divided by x^2-1.

   Mark one: **TRUE** or **FALSE**.

   Solution: Solution 1: Proof by contradiction. Assume that

$$p(x) = q(x)(x-1)+3,$$
$$p(x) = h(x)(x+1)+1, \text{ and}$$
$$p(x) = g(x)(x^2-1)+2x+1 = g(x)(x-1)(x+1)+2x+1.$$

for some polynomials $q(x)$, $h(x)$, and $g(x)$. Then plugging in $x = 1$ to the first equation, $p(1) = 3$ and plugging in $x = -1$ to the second equation, $p(-1) = 1$. From the third equation, if we plug in $x = 1$ we get $p(1) = 3$, and if we plug in $x = -1$, we get $p(-1) = -1$. But this contradicts that $p(-1) = 1$, since this would mean that $p(x)$ is not a polynomial function. Therefore the statement is false.

Solution 2: From the problem, we have

$$p(x) = q(x)(x-1)+3 \text{ and}$$
$$p(x) = h(x)(x+1)+1$$

for some polynomials $q(x)$ and $h(x)$, so we know $p(1) = 3$ and $p(-1) = 1$. We want to find $r(x)$ where

$$p(x) = g(x)(x^2-1)+r(x) = g(x)(x-1)(x+1)+r(x)$$

for some polynomial $g(x)$. We know that the degree of $r(x)$ is necessarily less than the degree of x^2-1, so the degree of $r(x)$ is at most 1. Therefore we can write $r(x) = ax+b$ and solve for a and b. We can write the equations

$$p(1) = r(1) = a+b = 3 \quad \text{and} \quad p(-1) = r(-1) = b-a = 1.$$

We can solve this by a simple substitution. From the second equation we can write $b = 1+a$, and substituting into the first, $2a+1 = 3$, so $a = 1$. Then substituting back into the second equation, $b-1 = 1$, so $b = 2$. Therefore the remainder must be $r(x) = x+2 \neq 2x+1$. Therefore the statement is false.

Common mistakes: Many students answered that the statement was false because x^2-1 is not coprime to $x+1$ and $x-1$, and therefore the Chinese Remainder Theorem can not be used. It is true that the Chinese Remainder Theorem can not be used on the three equations as stated in the problem, but as shown in Solution 2 above, this does not prevent us from determining the remainder of $p(x)$ divided by x^2-1. Another common mistake was stating that the statement was false based on some reasoning that the remainder of $p(x)$ divided by x^2-1 could not be of degree 1. Again, as shown in Solution 2 above, the remainder is indeed of degree 1, so this is not a valid line of reasoning.

4. **Secret Sharing**

Prof. Seshia would like to share a secret number s among us, where s could be any integer from 0 to 10. He chose a polynomial with degree 1 such that $P(0) \equiv s \pmod{11}$, but he only shared $P(1)$ with your GSI. Another key is on your hands. The way he distributed the second key $w = P(2)$ $(0 \leq w \leq 58)$ is by choosing a polynomial $Q(x)$ of degree ≤ 2 such that $Q(0) \equiv w \pmod{59}$. Here are your x and $Q(x)$:

Solution:

TAs please write a unique $Q(x_i) = y_i$ here in every student's worksheet based on function $Q(x) = x^2 + x + 7 \mod 59$:
$Q(1) = 9, Q(2) = 13, Q(3) = 19, Q(4) = 27, Q(5) = 37, Q(6) = 49, Q(7) = 4, Q(8) = 20, Q(9) = 38, Q(10) = 58, Q(11) = 21, Q(12) = 45, Q(13) = 12, Q(14) = 40, Q(15) = 11, Q(16) = 43, Q(17) = 18, Q(18) = 54, Q(19) = 33, Q(20) = 14, Q(21) = 56, Q(22) = 41, Q(23) = 28, Q(24) = 17, Q(25) = 8, Q(26) = 1, Q(27) = 55, Q(28) = 52, Q(29) = 51, Q(30) = 52, Q(31) = 55, Q(32) = 1, Q(33) = 8, Q(34) = 17, Q(35) = 28, Q(36) = 41, Q(37) = 56, Q(38) = 14, Q(39) = 33, Q(40) = 54, Q(41) = 18, Q(42) = 43, Q(43) = 11, Q(44) = 40, Q(45) = 12, Q(46) = 45, Q(47) = 21, Q(48) = 58, Q(49) = 38, Q(50) = 20$

(a) At least how many students would we need in order to find w?
Solution: 3.

(b) Please find w.
Solution: Let students work in groups of 3 or more to find the number. $w = 7$.

Maybe after they're done, mention that they actually only need a_0 to find $Q(0)$, and they can just calculate the terms that doesn't have x to save time.

(c) Please help your GSI find the secret number s.
Solution: GSI writes her/his number on board and lets them find s. For example, $P(1) = 6$, the polynomial will be $P(x) = x + 5 \mod 11$ and thus $s = 5$.

5. **Berlekamp–Welch algorithm**

In this question we will go through an example of error-correcting codes with general errors. We will send a message (m_0, m_1, m_2) of length $n = 3$. We will use an error-correcting code for $k = 1$ general error, doing arithmetic modulo 5.

(a) Suppose $(m_0, m_1, m_2) = (4, 3, 2)$. Use Lagrange interpolation to construct a polynomial $P(x)$ of degree 2 (remember all arithmetic is $\bmod 5$) so that $(P(0), P(1), P(2)) = (m_0, m_1, m_2)$. Then extend the message to lengeth $n + 2k$ by appending $P(3), P(4)$. What is the polynomial $P(x)$ and what is the message $(c_0, c_1, c_2, c_3, c_4) = (P(0), P(1), P(2), P(3), P(4))$ that is sent?

Solution: We use Lagrange interpolation to construct the unique quadratic polynomial $P(x)$ such that $P(0) = m_0 = 4, P(1) = m_1 = 3, P(2) = m_2 = 2$.

$$\begin{aligned}
\Delta_0(x) &= \frac{(x-1)(x-2)}{(0-1)(0-2)} = \frac{x^2 - 3x + 2}{2} \\
\Delta_1(x) &= \frac{(x-0)(x-2)}{(1-0)(1-2)} = \frac{x^2 - 2x}{-1} \\
\Delta_2(x) &= \frac{(x-0)(x-1)}{(2-0)(2-1)} = \frac{x^2 - x}{2} \\
P(x) &= m_0\Delta_0(x) + m_1\Delta_1(x) + m_2\Delta_2(x) \\
&= 4\Delta_0(x) + 3\Delta_1(x) + 2\Delta_2(x) \\
&= -x + 4
\end{aligned}$$

[Note that all arithmetic is $\bmod 5$, so for example $2^{-1} \equiv 3 \pmod 5$)]. Then we compute $P(3) = 1$ and $P(4) = 0$, so our message is 43210.

(b) Suppose the message is corrupted by changing c_0 to 0. We will locate the error using the Berlekamp–Welsh method. Let $E(x) = x + b_0$ be the error-locator polynomial, and $Q(x) = P(x)E(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ be a polynomial with unknown coefficients. Write down the system of linear equations (involving unknowns a_0, a_1, a_2, a_3, b_0) in the Berlekamp–Welsh method. You need not solve the equations.

Solution: The message received is $(c_0', c_1', c_2', c_3', c_4') = (0,3,2,1,0)$. Let $R(x)$ be the function such $R(i) = c_i'$ for $0 \le i < 5$. Let $E(x) = x + b_0$ be the error-locator polynomial, and $Q(x) = P(x)E(x) = a_3x^3 + a_2x^2 + a_1x + a_0$. Since $Q(i) = P(i)E(i) = R(i)E(i)$ for $1 \le i < 5$, we have the following equalities $\pmod 5$:

$$\begin{aligned} Q(0) &= 0E(0) \\ Q(1) &= 3E(1) \\ Q(2) &= 2E(2) \\ Q(3) &= 1E(3) \\ Q(4) &= 0E(4) \end{aligned}$$

They lead to the following system of linear equations:

$$\begin{array}{rcrcrcrcrcr} & & & & & & a_0 & & & = & 0 \\ a_3 & + & a_2 & + & a_1 & + & a_0 & - & 3b_0 & = & 3 \\ 8a_3 & + & 4a_2 & + & 2a_1 & + & a_0 & - & 2b_0 & = & 4 \\ 27a_3 & + & 9a_2 & + & 3a_1 & + & a_0 & - & b_0 & = & 3 \\ 64a_3 & + & 16a_2 & + & 4a_1 & + & a_0 & & & = & 0 \end{array}$$

(c) The solution to the equations in part (b) is $b_0 = 0, a_0 = 0, a_1 = 4, a_2 = 4, a_3 = 0$. Show how the recipient can recover the original message (m_0, m_1, m_2).

Solution: From the solution, we know

$$\begin{aligned} Q(x) &= a_3x^3 + a_2x^2 + a_1x + a_0 = -x^2 + 4x \\ E(x) &= x + b_0 = x \end{aligned}$$

Since $Q(x) = P(x)E(x)$, the recipient can compute $P(x) = Q(x)/E(x) = -x + 4$ [note that this is the same polynomial $P(x)$ from part (a) used by the sender]. The recipient may deduce the location of the error from $E(x)$ as follows. There is only one error at location e_1, we have $E(x) = (x - e_1) = x$, so $e_1 = 0$ and the error is at position 0. To correct the error we evaluate $P(0) = 4$. Since the other two positions m_1, m_2 of the message are uncorrupted, we recover the original message $(m_0, m_1, m_2) = (4, 3, 2)$.