1 Equivalent Polynomials

Note 7
Note 8

This problem is about polynomials with coefficients in GF(p) for some prime $p \in \mathbb{N}$. We say that two such polynomials f and g are *equivalent* if $f(x) \equiv g(x) \pmod{p}$ for every $x \in \text{GF}(p)$.

(a) Show that $f(x) = x^{p-1}$ and $g(x) = 1$ are **not** equivalent polynomials under GF(p).

(b) Use Fermat's Little Theorem to find a polynomial with degree strictly less than 5 that is equivalent to $f(x) = x^5$ over GF(5); then find a polynomial with degree strictly less than 11 that is equivalent to $g(x) = 4x^{70} + 9x^{11} + 3$ over GF(11).

(c) In GF(p), prove that whenever $f(x)$ has degree $\geq p$, it is equivalent to some polynomial $\tilde{f}(x)$ with degree $< p$.

Solution:

(a) For f and g to be equivalent, they must satisfy $f(x) \equiv g(x) \pmod{p}$ for all values of x, including zero. But $f(0) \equiv 0 \pmod{p}$ and $g(0) \equiv 1 \pmod{p}$, so they are not equivalent.

(b) Fermat's Little Theorem says that for any nonzero integer a and any prime number p, $a^{p-1} \equiv 1 \mod p$. We're allowed to multiply through by a, so the theorem is equivalent to saying that $a^p \equiv a \mod p$; note that this is true even when $a = 0$, since in that case we just have $0^p \equiv 0 \pmod{p}$.

The problem asks for a polynomial $\tilde{f}(x)$, different from $f(x)$, with the property that $\tilde{f}(a) \equiv a^5 \mod 5$ for any integer a. Directly using the theorem, $\tilde{f}(x) = x$ will work. We can do something similar with $g(x) = 4x^{70} + 9x^{11} + 3$ modulo 11; since $x^{11} \equiv x \pmod{11}$, we repeatedly substitute x^{11} with x, effectively reducing the exponent by 10. We can only do this as long as the exponent remains greater than or equal to 11, so we end up with $\tilde{g}(x) = 4x^{10} + 9x + 3$.

(c) One proof uses Fermat's Little Theorem. As a warm-up, let $d \geq p$; we'll find a polynomial equivalent to x^d. For any integer, we know

$$\begin{aligned} a^d &= a^{d-p}a^p \\ &\equiv a^{d-p}a \pmod{p} \\ &\equiv a^{d-p+1} \pmod{p}. \end{aligned}$$

In other words x^d is equivalent to the polynomial $x^{d-(p-1)}$. If $d - (p-1) \geq q$, we can show in the same way that x^d is equivalent to $x^{d-2(p-1)}$. Since we subtract $p-1$ every time, the sequence $d, d-(p-1), d-2(p-1), \ldots$ must eventually be smaller than p. Now if $f(x)$ is any polynomial with degree $\geq p$, we can apply this same trick to every x^k that appears for which $k \geq p$.

Another proof uses Lagrange interpolation. Let $f(x)$ have degree $\geq p$. By Lagrange interpolation, there is a unique polynomial $\tilde{f}(x)$ of degree at most $p-1$ passing through the points $(0, f(0)), (1, f(1)), (2, f(2)), \ldots, (p-1, f(p-1))$, and we know it must be equivalent to $f(x)$ because f also passes through the same p points.

2 Secret Sharing

Note 8

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

- Two TAs together should be able to access the answers
- Three Readers together should be able to access the answers
- One TA and one Reader together should also be able to access the answers
- One TA by themself or two Readers by themselves should not be able to access the answers.

Design a Secret Sharing scheme to make this work.

Solution:

Solution 1 We can use a degree 2 polynomial, which is uniquely determined by 3 points. Evaluate the polynomial at 7 points, and distribute a point to each Reader and 2 points to each TA. Then, all possible combinations will have at least 3 points to recover the answer key.

Basically, the point of this problem is to assign different weight to different class of people. If we give one share to everyone, then 2 Readers can also recover the secret and the scheme is broken.

Solution 2 We construct three polynomials, one for each way of recovering the answer key:

- A degree 1 polynomial for recovering with two TAs, evaluated at 2 points. Distribute a point to each TA.
- A degree 2 polynomial for recovering with three readers, evaluated at 3 points. Distribute a point to each Reader.
- A degree 1 polynomial for recovering with one TA + one reader. Evaluate this polynomial at 2 points, and distribute one point to all TAs and one point to all readers.

All combinations can then use the corresponding polynomial to recover the answer key.

3 One Point Interpolation

Note 8 Suppose we have a polynomial $f(x) = x^k + c_{k-1}x^{k-1} + \cdots + c_2x^2 + c_1x + c_0$.

(a) Can we determine $f(x)$ with k points? If so, provide a set of inputs $x_0, x_1, \ldots, x_{k-1}$ such that knowing points $(x_0, f(x_0)), (x_1, f(x_1)), \ldots, (x_{k-1}, f(x_{k-1}))$ allows us to uniquely determine $f(x)$, and show how $f(x)$ can be determined from such points. If not, provide a proof of why this is not possible.

(b) Now, assume each coefficient is an integer satisfying $0 \le c_i < 100 \quad \forall i \in [0, k-1]$. Can we determine $f(x)$ with one point? If so, provide an input x_* such that knowing the point $(x_*, f(x_*))$ allows us to uniquely determine $f(x)$, and show how $f(x)$ can be determined from this point. If not, provide a proof of why this is not possible.

Solution:

(a) Yes. Since the leading coefficient is 1, we only need to find the k remaining coefficients $c_0, c_1, \ldots, c_{k-1}$ to determine $f(x)$. This can be done with *any* k distinct points.

For example, suppose we know the points $(0, f(0)), (1, f(1)), \ldots, (k-1, f(k-1))$. We can then write the degree $k-1$ polynomial

$$g(x) = c_{k-1}x^{k-1} + \cdots + c_2x^2 + c_1x + c_0 = f(x) - x^k$$

which can be determined via Lagrange interpolation on $(0, f(0)), (1, f(1) - 1), (2, f(2) - 2^k)$, $\ldots, (k-1, f(k-1) - (k-1)^k)$, uniquely yielding our desired coefficients $c_0, c_1, \ldots, c_{k-1}$.

(b) Yes. We can express each nonnegative two-digit integer $c_i = 10d_{2i+1} + d_{2i}$ for digits $d_i \in [0, 9]$.

Using $x_* = 100$,

$$\begin{aligned} f(100) &= 100^k + c_{k-1}100^{k-1} + \cdots + c_2 100^2 + c_1 100 + c_0 \\ &= 10^{2k} + (10d_{2k-1} + d_{2k-2})10^{2k-2} + \cdots + (10d_5 + d_4)10^4 + (10d_3 + d_2)10^2 + (10d_1 + d_0) \\ &= 10^{2k} + 10^{2k-1}d_{2k-1} + 10^{2k-2}d_{2k-2} + \cdots + 10^5 d_5 + 10^4 d_4 + 10^3 d_3 + 10^2 d_2 + 10 d_1 + d_0 \end{aligned}$$

Thus, the rightmost $2k-1$ digits of $f(100)$, from right to left, are $d_0, d_1, \ldots, d_{2k-1}$; we can then determine our desired coefficients $c_i = 10d_{2i+1} + d_{2i}$.

4 Error-Correcting Codes

Note 9 (a) Recall from class the error-correcting code for erasure errors, which protects against up to k lost packets by sending a total of $n+k$ packets (where n is the number of packets in the original message). Often the number of packets lost is not some fixed number k, but rather a *fraction* of the number of packets sent. Suppose we wish to protect against a fraction α of lost packets (where $0 < \alpha < 1$). At least how many packets do we need to send (as a function of n and α)?

(b) Repeat part (a) for the case of general errors.

Solution:

(a) Suppose we send a total of m packets (where m is to be determined). Since at most a fraction α of these are lost, the number of packets received is at least $(1-\alpha)m$. But in order to reconstruct the polynomial used in transmission, we need at least n packets. Hence it is sufficient to have $(1-\alpha)m \geq n$, which can be rearranged to give $m \geq n/(1-\alpha)$.

(b) Suppose we send a total of $m = n+2k$ packets, where k is the number of errors we can guard against. The number of corrupted packets is at most αm, so we need $k \geq \alpha m$. Hence $m \geq n + 2\alpha m$. Rearranging gives $m \geq n/(1-2\alpha)$.

Note: Recovery in this case is impossible if $\alpha \geq 1/2$.

5 Alice and Bob

Note 8
Note 9

(a) Alice decides that instead of encoding her message as the values of a polynomial, she will encode her message as the coefficients of a degree 2 polynomial $P(x)$. For her message $[m_1, m_2, m_3]$, she creates the polynomial $P(x) = m_1x^2 + m_2x + m_3$ and sends the five packets $(0, P(0))$, $(1, P(1))$, $(2, P(2))$, $(3, P(3))$, and $(4, P(4))$ to Bob. However, one of the packet y-values (one of the $P(i)$ terms; the second attribute in the pair) is changed by Eve before it reaches Bob. If Bob receives

$$(0,1),(1,3),(2,0),(3,1),(4,0)$$

and knows Alice's encoding scheme and that Eve changed one of the packets, can he recover the original message? If so, find it as well as the x-value of the packet that Eve changed. If he can't, explain why. Work in mod 7. Also, feel free to use a calculator or online systems of equations solver, but make sure it can work under mod 7.

(b) Bob gets tired of decoding degree 2 polynomials. He convinces Alice to encode her messages on a degree 1 polynomial. Alice, just to be safe, continues to send 5 points on her polynomial even though it is only degree 1. She makes sure to choose her message so that it can be encoded on a degree 1 polynomial. However, Eve changes two of the packets. Bob receives $(0,5)$, $(1,7)$, $(2,x)$, $(3,5)$, $(4,0)$. If Alice sent $(0,5)$, $(1,7)$, $(2,9)$, $(3,-2)$, $(4,0)$, for what values of x will Bob not uniquely be able to determine Alice's message? Assume that Bob knows Eve changed two packets. Work in mod 13. Again, feel free to use a calculator or graphing calculator software.

(c) Alice wants to send a length n message to Bob. There are two communication channels available to her: Channel X and Channel Y. Only 6 packets can be sent through channel X. Similarly, Channel Y will only deliver 6 packets, but it will also corrupt (change the value) of one of the delivered packets. Using each of the two channels once, what is the largest message length n such that Bob so that he can always reconstruct the message?

Solution:

(a) We can use Berlekamp and Welch. We have: $Q(x) = P(x)E(x)$. $E(x)$ has degree 1 since we know we have at most 1 error. $Q(x)$ is degree 3 since $P(x)$ is degree 2. We can write a system of linear equations and solve for the coefficients of $Q(x) = ax^3 + bx^2 + cx + d$ and $E(x) = (x - e)$ by writing the equation $Q(i) = r_i \cdot E(i)$ for $0 \le i \le 4$, where r_i is the ith received point.

$$\begin{aligned} d &= 1(0-e) \\ a+b+c+d &= 3(1-e) \\ 8a+4b+2c+d &= 0(2-e) \\ 27a+9b+3c+d &= 1(3-e) \\ 64a+16b+4c+d &= 0(4-e) \end{aligned}$$

Since we are working in mod 7, this is equivalent to:

$$\begin{aligned} d &= -e \\ a+b+c+d &= 3-3e \\ a+4b+2c+d &= 0 \\ 6a+2b+3c+d &= 3-e \\ a+2b+4c+d &= 0 \end{aligned}$$

Solving yields:

$$Q(x) = x^3 + 5x^2 + 5x + 4, E(x) = x - 3$$

To find $P(x)$ we divide $Q(x)$ by $E(x)$ and get $P(x) = x^2 + x + 1$. So Alice's message is $m_1 = 1, m_2 = 1, m_3 = 1$. The x-value of the packet Eve changed is 3.

Alternative solution: Since we have 5 points, we have to find a polynomial of degree 2 that goes through 4 of those points. The point that the polynomial does not go through will be the packet that Eve changed. Since 3 points uniquely determine a polynomial of degree 2, we can pick 3 points and check if it goes through a 4th point. (It may be the case that we need to try all sets of 3 points.)

We pick the points $(1,3), (2,0), (4,0)$. Lagrange interpolation can be used to create the polynomial but we can see that for the polynomial that goes through these 3 points, it has 0s at $x = 2$ and $x = 4$. Thus the polynomial is $k(x-2)(x-4) = k(x^2 - 6x + 8) \pmod 7 \equiv k(x^2 + x + 1) \pmod 7$. We find $k \equiv 1$ by plugging in the point $(1,3)$, so our polynomial is $x^2 + x + 1$. We then check to see if this polynomial goes through one of the 2 points that we didn't use. Plugging in 0 for x, we get 1. The packet that Eve changed is the point that our polynomial does not go through which has x-value 3. Alice's original message was $m_1 = 1, m_2 = 1, m_3 = 1$.

(b) Since Bob knows that Eve changed 2 of the points, the 3 remaining points will still be on the degree 1 polynomial that Alice encoded her message on. Thus if Bob can find a degree 1 polynomial that passes through at least 3 of the points that he receives, he will be able to uniquely recover Eve's message. The only time that Bob cannot uniquely determine Alice's message is if there are 2 polynomials with degree 1 that pass through 3 of the 5 points that he receives. Since we are working with degree 1 polynomials, we can plot the points that Bob receives and then see which values of x will cause 2 sets of 3 points to fall on a line. $(0,5),(1,7),(4,0)$ already fall on a line. If $x = 6$, $(1,7),(2,6),(3,5)$ also falls on a line. If $x = 5$, $(0,5),(2,5),(3,5)$ also falls on a line. If $x = 9$, $(0,5),(2,9),(4,0)$ falls on the original line, so here Bob can decode the message. If $x = 10$, $(2,10),(3,5),(4,0)$ also falls on a line. So if $x = 6,5,10$, Bob will not be able to uniquely determine Alice's message.

(c) Channel X can send 6 packets, so the first 6 characters of the message can be send through Channel X. Channel Y can send 6 packets, but 1 will be corrupted, thus only a message of length 4 can be sent. Thus, a total of $m = 6+4 = 10$ characters can effectively sent.