1 Interpolation practice

Find a polynomial $h(x) = ax^2 + bx + c$ of degree at most 2 such that $h(0) \equiv 3 \pmod 7$, $h(1) \equiv 6 \pmod 7$, and $h(2) \equiv 6 \pmod 7$ with Lagrange Polynomials.

How many degree (at most) 2 polynomials $h(x)$ are there with $h(0) \equiv 3 \pmod 7$ and $h(1) \equiv 6 \pmod 7$?

–Solution–

The polynomial: $h(x) = 2x^2 + x + 3 \mod 7$.
There are 7 possible polynomials: Three points uniquely determine a degree at most 2 polynomial. With 2 points specified, one point is free, for which there are 7 possible values.

–Exemplar–

1. $p_0(x) = (x-1)(x-2) = x^2 - 3x + 2 \equiv x^2 + 4x + 2 \mod 7$. $p_0(0) = 2$. $2^{-1} \equiv 4 \mod 7$.
   $\Delta_0(x) = 4x^2 + 2x + 1$.
2. $p_1(x) = x(x-2) = x^2 - 2x \equiv x^2 + 5x \mod 7$. $p_1(1) = 6$. $6^{-1} \equiv 6 \mod 7$.
   $\Delta_1(x) = 6x^2 + 2x$.
3. $p_2(x) = x(x-1) = x^2 - x \equiv x^2 + 6x \mod 7$. $p_2(2) = 2$.
   $\Delta_2(x) = 4x^2 + 3x$.

$h(x) = 3\Delta_0(x) + 6\Delta_1(x) + 6\Delta_2(x) = (5x^2 + 6x + 3) + (x^2 + 5x) + (3x^2 + 4x) = 2x^2 + x + 3$.

$$h(x) = 2x^2 + x + 3 \mod 7$$

3 points uniquely determine a degree 2 polynomial. For the third point, there are 7 choices, in $GF(7)$. Thus, $\boxed{\text{there are 7 distinct degree (at most) 2 polynomials}}$ satisfying $h(0) \equiv 3 \mod 7$ and $h(1) \equiv 6 \mod 7$.

2 Error-correcting codes

In this question we will go through an example of error-correcting codes. Since we will do this by hand, the message we will send is going to be short, consisting of $n = 3$ numbers, each modulo 5, and the number of errors we can correct is at most $k = 1$ errors.

(a) First, construct the message. Let $a_0 = 3$, $a_1 = 4$, and $a_2 = 2$; use the polynomial interpolation formula to construct a polynomial $P(x)$ of degree 2 (remember that all arithmetic is mod 5) so that $P(0) = a_0$, $P(1) = a_1$, and $P(2) = a_2$; then extend the message to length $n + 2k$ by adding $P(3)$ and $P(4)$. What is the polynomial $P(x)$ and what is the message that is sent?

–Solution–

$$P(x) = x^2 + 3 \mod 5$$

The message sent is: $[3, 4, 2, 2, 4]$.

–Exemplar–

(I) $p_0(x) = x^2 - 3x + 2 \equiv x^2 + 2x + 2 \mod 5$. $p_0(0) = 2$, inverse is 3.
$\Delta_0(x) = 3x^2 + x + 1$.

(II) $p_1(x) = x^2 - 2x \equiv x^2 + 3x \mod 5$. $p_1(1) = 4$, inverse is 4.
$\Delta_1(x) = 4x^2 + 2x$.

(III) $p_2(x) = x^2 - x \equiv x^2 + 4x \mod 5$. $p_2(2) = 2$.
$\Delta_2(x) = 3x^2 + 2x$.

$$P(x) = (4x^2 + 3x + 3) + (x^2 + 3x) + (x^2 + 4x) = x^2 + 0x + 3 \mod 5$$

$P(3) = 2$, $P(4) = 4$.
The message is : $[P(0), P(1), P(2), P(3), P(4)] = [3, 4, 2, 2, 4]$

(b) Suppose the message is corrupted by changing a_0 to 0. Use the Berlekamp-Welsh method to detect the location of the error and to reconstruct the original message $a_0a_1a_2$. Show clearly all your work.

–Solution & Exemplar–

The modified message is $m' = [0, 4, 2, 2, 4]$.
Only one error, so the error-locator polynomial is: $E(x) = x + b_0$.
$P(x)E(x) = Q(x)$, so $Q(x) = a_3x^3 + a_2x^2 + a_1x + a_0$.

$$\begin{aligned}
Q(0) = a_0 &= R(0)E(0) = 0 \\
Q(1) = a_3 + a_2 + a_1 + a_0 &= R(1)E(1) = 4 + 4b_0 \\
Q(2) = 3a_3 + 4a_2 + 2a_1 + a_0 &= R(2)E(2) = 2(2 + b_0) = 4 + 2b_0 \\
Q(3) = 2a_3 + 4a_2 + 3a_1 + a_0 &= R(3)E(3) = 2(3 + b_0) = 1 + 2b_0 \\
Q(4) = 4a_3 + a_2 + 4a_1 + a_0 &= R(4)E(4) = 4(4 + b_0) = 1 + 4b_0
\end{aligned}$$

$$\begin{aligned}
a_0 &= 0 \\
a_3 + a_2 + a_1 + a_0 + b_0 &= 4 \\
3a_3 + 4a_2 + 2a_1 + a_0 + 3b_0 &= 4 \\
2a_3 + 4a_3 + 3a_1 + a_0 + 3b_0 &= 1 \\
4a_3 + a_2 + 4a_1 + a_0 + b_0 &= 1
\end{aligned}$$

So, $a_0 = 0$, and we solve for the remaining variables with Gaussian elimination.

$$\left[\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 4 \\ 3 & 4 & 2 & 3 & 4 \\ 2 & 4 & 3 & 3 & 1 \\ 4 & 1 & 4 & 1 & 1 \end{array}\right] \Rightarrow \begin{array}{c} v_1 \\ +2v_1 \\ +3v_1 \\ +v_1 \end{array} \left[\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 4 \\ 0 & 1 & 4 & 0 & 2 \\ 0 & 2 & 1 & 1 & 3 \\ 0 & 2 & 0 & 2 & 0 \end{array}\right] \Rightarrow \begin{array}{c} \\ v_2 \\ +3v_2 \\ +3v_2 \end{array} \left[\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 4 \\ 0 & 1 & 4 & 0 & 2 \\ 0 & 0 & 3 & 1 & 4 \\ 0 & 0 & 2 & 2 & 1 \end{array}\right]$$

Inverse of 3 is 2, so third row is [0 0 1 2 | 3].

$$\Rightarrow \begin{array}{c} \\ \\ v_3 \\ +3v_3 \end{array} \left[\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 4 \\ 0 & 1 & 4 & 0 & 2 \\ 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 3 & 0 \end{array}\right] \Rightarrow \begin{array}{c} \\ \\ \\ 3^{-1} \end{array} \left[\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 4 \\ 0 & 1 & 4 & 0 & 2 \\ 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right] \Rightarrow \begin{array}{c} +4v_4 \\ \\ +3v_4 \\ v_4 \end{array} \left[\begin{array}{cccc|c} 1 & 1 & 1 & 0 & 4 \\ 0 & 1 & 4 & 0 & 2 \\ 0 & 0 & 1 & 0 & 3 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right]$$

$$\Rightarrow \begin{array}{c} +4v_3 \\ +v_3 \\ v_3 \\ \\ \end{array} \left[\begin{array}{cccc|c} 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 3 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right] \Rightarrow \begin{array}{c} +4v_2 \\ v_2 \\ \\ \\ \end{array} \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 3 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right]$$

Finally, $a_3 = 1$, $a_2 = 0$, $a_1 = 3$, $a_0 = 0$, and $b_0 = 0$.

Therefore, $Q(x) = x^3 + 3x$, and $E(x) = x$. $P(x) = \frac{Q(x)}{E(x)} = x^2 + 3$, which is precisely our original polynomial.
Because $E(x) = x$, we know the error occurred at 0, so $P(0) = 3$ allows us to reconstruct the original message.

3 List decoding

Consider a n character message encoded into m characters over the field $GF(p)$ using polynomials. Consider that one receives $n-1$ of the m characters. It is clearly impossible to find a unique reconstruction of the original n-character message. However, it is possible to find a list of size at most p possible candidates for the message, given the $n-1$ received characters. Give such a method to find a list of candidate messages.

–Solution–

The message is encoded with a polynomial of degree at most $n-1$. For each character $c \in [0, p-1]$ (all possible values of a character):

(i) Append c to the received message. Virtual message length n, can find degree $n-1$ polynomial.

(ii) Use Lagrangian interpolation to reconstruct candidate message, add message to list.

Thus, there are at most p possible messages.

–Solution & Exemplar–

Assuming there are no errors in the channel, we have $n-1$ distinct points from which to infer a degree $n-1$ polynomial (as a message of length n is encoded as a degree $n-1$ polynomial). n points are required to uniquely identify a degree $n-1$ polynomial. With those fixed, there are p possible values for the final point of the polynomial, making at most p distinct polynomials sharing the $n-1$ points received in the message. Therefore, we can simply add in "virtual" points for one of the packets we missed, and use Lagrangian interpolation to determine up to p distinct polynomials of degree $n-1$.

4 Secret Sharing.

Suppose that the staff at a company includes three managers and four secretaries. A company has a secret it needs to protect. This secret should only be accessible by any two managers, or by any manager in conjunction with 3 secretaries. Any smaller group, or even a group of the four secretaries by themselves, will get no information about the secret.

Design such a secret-sharing scheme.

–Solution–

Create a degree 5 polynomial $P(x)$, and let the secret be $s = P(0)$. Generate shares $P(1), P(2), \ldots, P(13)$. Distribute 3 to each manager and one to each secretary.
Then, a group of one manager and 3 secretaries has 6 points, and a group of two managers has 6 points, enough to reconstruct $P(x)$ and find $s = P(0)$.

–Exemplar–

3 secretaries should be able to take the place of a single manager in the secret sharing scheme. Let the secret $s = P(0)$, where $P(x)$ is a degree 5 polynomial. Generate shares $P(1), P(2), \ldots, P(13)$. Distribute 3 to each manager and 1 to each secretary.
Six points are necessary to uniquely reconstruct $P(x)$. A group of two managers or a group of one manager with three secretaries each have 6 shares, enough to reconstruct $P(x)$ and discover $s = P(0)$.
Alone, all four secretaries only have 4 shares, and any manager with less than 3 secretaries has less than 6 shares.