1 Interpol Warning

Consider the set of four points $\{(-1,1),(0,2),(1,5),(2,40)\}$.

Find the unique polynomial over $\mathbb{R}$ of degree ≤ 3 that passes through these points by either solving a system of linear equations or by Lagrange Interpolation.

Solution:

We first find the polynomial by solving a system of linear equations. Suppose that the desired polynomial is of the form ax^3+bx^2+cx+d. Then using the given points, we have:

$$\begin{aligned} -a+b-c+d &= 1 \\ d &= 2 \\ a+b+c+d &= 5 \\ 8a+4b+2c+d &= 40 \end{aligned}$$

Solving this system (using standard simultaneous linear equation techniques, such as elimination or substitution) gives $a=5, b=1, c=-3, d=2$. Therefore the polynomial is $5x^3+x^2-3x+2$.

We now find the polynomial using Lagrange Interpolation. We construct the following delta functions:

$$\begin{aligned} \Delta_{-1}(x) &= \frac{x(x-1)(x-2)}{(-1)(-1-1)(-1-2)} = -\frac{1}{6}(x^3-3x^2+2x) \\ \Delta_0(x) &= \frac{(x+1)(x-1)(x-2)}{(1)(-1)(-2)} = \frac{1}{2}(x^3-2x^2-x+2) \\ \Delta_1(x) &= \frac{(x+1)(x)(x-2)}{(1+1)(1)(1-2)} = -\frac{1}{2}(x^3-x^2-2x) \\ \Delta_2(x) &= \frac{(x+1)(x)(x-1)}{(2+1)(2)(2-1)} = \frac{1}{6}(x^3-x) \end{aligned}$$

Our desired polynomial is equal to

$$\Delta_{-1}(x)+2\Delta_0(x)+5\Delta_1(x)+40\Delta_2(x) = 5x^3+x^2-3x+2.$$

As can be seen, both techniques yield the same answer.

2 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 $s \in \mathbb{Z}$. 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.

Solution:

(a) Create a polynomial of degree $n-1$ and give each country one point. Give the Secretary General $n-m$ points, so that if he collaborates with m countries, they will have $n-m+m=n$ points and can reconstruct the polynomial. Without the General, n countries can come together and also recover the polynomial. No combination of the General with fewer than m countries can recover the polynomial.

Alternatively, we can have two schemes, one for each condition. For the first condition: just one polynomial of degree $\leq n-1$ would do, where each country gets one point. The polynomial evaluated at 0 would give the secret. For the second condition: one polynomial is created of degree $m-1$ and a point is given to each country. Another polynomial of degree 1 is created, where one point is given to the secretary general and the second point can be constructed from the first polynomial if m or more of the countries come together. With these two points, we have a unique 1-degree polynomial, which could give the secret evaluated at 0.

(b) The scheme in part (a) remains the same, but instead of directly giving each country a point on the $n-1$ degree polynomial to open the vault, construct an additional polynomial for each country that will produce that point.

Each country's polynomial has degree $k-1$, and a point is given to each of the k representatives of the country. Thus, when they all get together they can produce a point for either of the schemes.

3 Erasure Warm-Up

Working over $GF(q)$, you want to send your friend a message of $n=4$ packets and guard against 2 lost packets. What is the minimum q you can use? What is the maximum degree of the unique polynomial that describes your message?

Solution:

To guard against 2 lost packets, you want to send $4+2=6$ packets. Since we want q prime, the minimum it can be is 7. Since you have 4 points, your polynomial needs to be degree 3.

Note: Encoding our message in $GF(7)$ requires that our message is not larger than 6.