CS 70 Discrete Mathematics and Probability Theory
Spring 2015 Vazirani Discussion 7M

1. Sanity Check!

1. What's the minimum number of roots of a degree 4 real polynomial?

   Answer: 0, for example x^4+1

2. What's the minimum number of roots of a degree 5 real polynomial?

   Answer: 1, the polynomial must pass through the x-axis at least once since it is an odd function.

3. What's the minimum number of roots of a degree 5 polynomial in GF(7)?

   Answer: 0, For example x^5-x+1 is zero nowhere.

4. How many degree at most 3 polynomials are there in GF(7)?

   Answer: Each polynomial can be written as ax^3+bx^2+cx+d, so there are 7^4 polynomials.

2. Lagrange Interpolation

Find a unique real polynomial $p(x)$ of degree at most 3 that passes through points $(-1,3)$, $(0,1)$, $(1,2)$, and $(2,0)$ using Lagrange interpolation.

1. Find $\Delta_{-1}(x)$ where $\Delta_{-1}(0)=\Delta_{-1}(1)=\Delta_{-1}(2)=0$ and $\Delta_{-1}(-1)=1$.

   Answer: $\Delta_{-1}(x)=\frac{x(x-1)(x-2)}{-6}$

2. Find $\Delta_0(x)$ where $\Delta_0(-1)=\Delta_0(1)=\Delta_0(2)=0$ and $\Delta_0(0)=1$.

   Answer: $\Delta_0(x)=\frac{(x+1)(x-1)(x-2)}{2}$

3. Find $\Delta_1(x)$ where $\Delta_1(-1)=\Delta_1(0)=\Delta_1(2)=0$ and $\Delta_1(1)=1$.

   Answer: $\Delta_1(x)=\frac{(x+1)(x)(x-2)}{-2}$.

4. Find $\Delta_2(x)$ where $\Delta_2(-1)=\Delta_2(0)=\Delta_2(1)=0$ and $\Delta_2(2)=1$.

   Answer: $\Delta_2(x)=\frac{(x+1)(x)(x-1)}{6}$.

5. Construct $p(x)$ using a linear combination of $\Delta_{-1}(x)$, $\Delta_0(x)$, $\Delta_1(x)$ and $\Delta_2(x)$.

   Answer: We don't need $\Delta_2(x)$.
   $p(x)=3\cdot\Delta_{-1}(x)+1\cdot\Delta_0(x)+2\cdot\Delta_1(x)+0\cdot\Delta_2(x)$.

3. Secret Sharing

Umesh wants to share a secret among 4 TAs and 14 readers, such that a subset of them can reconstruct the secret iff it contains either (i) at least 2 TAs, or (ii) at least 1 TA and at least 2 readers, or (iii) at least 4 readers. Explain how this can be accomplished.

Answer: First note that in this case, a TA essentially counts as 2 readers. Thus, we make a polynomial p of degree 3 such that $p(0)=s$, where s is Tom's secret. Each reader gets one point in p, while each TA gets 2. Thus, if either 2 TAs, 1 TA and 2 readers, or 4 readers collaborate, they can recover s.

4. 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?

Answer:

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.