CS 70 FALL 2006 — DISCUSSION #5

D. GARMIRE, L. ORECCHIA & B. RUBINSTEIN

1. Administrivia

(1) Course Information
  - The fifth homework is due September 29^{th} at 4pm in 283 Soda Hall.

(2) Discussion Information
  - Homework #3 is graded and will be handed out this section.

2. Polynomials on the Reals

Briefly, recall the following polynomial basics.

Definition 1. A *polynomial of degree* d on the reals is a function $p(x) = a_0 + a_1x^1 + a_2x^2 + \ldots + a_dx^d$, where the input variable x and the $d+1$ constants $a_0, \ldots, a_d$ are all real numbers, and additionally $a_d \neq 0$. r is a *root* of polynomial $p(x)$ if $p(r) = 0$.

Theorem 2. *Over the reals:*

(1) A degree d polynomial has at most d roots.
(2) For any $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1}) \in \mathbb{R}^2$ there exists a unique polynomial $p(x)$ of degree at most d such that $p(x_i) = y_i$, for each $1 \leq i \leq d+1$.

Exercise 1. Find (and prove) an upper-bound on the number of times two degree d polynomials can intersect. What if the polynomials' degrees differ?

3. Polynomial Interpolation on the Reals

Property 2 (see Theorem 2) says that any set of $d+1$ points $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1}) \in \mathbb{R}^2$ can be interpolated by a polynomial of degree at most d. But how can we efficiently perform such an interpolation? In lecture we saw that the Lagrange interpolation method achieves this feat.

Method 3. The Lagrange interpolation procedure:

i. $q_i(x) = \prod_{\substack{j=1 \\ j \neq i}}^{d+1} (x - x_j)$ is a degree d polynomial satisfying $q_i(x_j) = 0$ for all $j \neq i$ and $q_i(x_i)$ is some non-zero constant;
ii. $\Delta_i(x) = \frac{q_i(x)}{q_i(x_i)}$ is a degree d polynomial equal to 1 at x_i and 0 on the x_j with $j \neq i$;
iii. $y_i\Delta_i(x)$ is a degree d polynomial equal to y_i at x_i and 0 on the x_j with $j \neq i$; and
iv. $p(x) = \sum_{i=1}^{d+1} y_i\Delta_i(x)$ is a polynomial of degree at most d that satisfies $p(x_i) = y_i$ for each $1 \leq i \leq d+1$ (i.e. witnessing Property 2 as desired).

Date: September 27, 2006.

The authors gratefully acknowledge Chris Crutchfield and Amir Kamil for the use of their previous notes, which form part of the basis for this handout.

Exercise 2. Use the Lagrange interpolation method to determine the polynomial of degree at most 3 that fits the points $(-1,2),(0,1),(1,2),(2,5)$. What is the (exact) degree of this polynomial?

4. From Reals to Fields (e.g. $\mathbb{F}_m$)

Let's start with a formal definition of a field for concreteness (don't worry, we're not going to be too formal today!).

Definition 4. Let $\mathbb{F}$ be a set endowed with binary operators[1] $+$ and $\times$. Then $\mathbb{F}$ is a *field* if, for all $a,b,c \in \mathbb{F}$,

(i) *(Closure)* $a+b \in \mathbb{F}$ and $a \times b \in \mathbb{F}$;
(ii) *(Associativity)* $a+(b+c) = (a+b)+c$ and $a \times (b \times c) = (a \times b) \times c$;
(iii) *(Commutativity)* $a+b = b+a$ and $a \times b = b \times a$;
(iv) *(Distributivity)* $a \times (b+c) = (a \times b) + (a \times c)$;
(v) *(Identities)* there exist elements $0, 1 \in \mathbb{F}$ such that $a+0=a$ and $a \times 1 = a$; and
(vi) *(Inverses)* there exists element $-a \in \mathbb{F}$ such that $a+(-a)=0$, and if $a \neq 0$ then there exists element $a^{-1} \in \mathbb{F}$ such that $a \times a^{-1} = 1$.

Example 5. Valid fields include (all with $+$ as addition and $\times$ as multiplication):
(a) The reals $\mathbb{R}$;
(b) The rationals $\mathbb{Q} = \left\{\frac{p}{q} \mid p,q \in \mathbb{Z}, q \neq 0\right\}$; and
(c) The integers modulo a prime m, denoted $\mathbb{F}_m$

Invalid fields include:
(d) The integers $\mathbb{Z}$ since there exists no multiplicative inverse for, e.g., 2; and
(e) The integers modulo a composite[2] n denoted $\mathbb{Z}_n$ since the prime factors of n have no multiplicative inverse.

The facts that polynomials make sense on the reals and that the two fundamental properties hold for polynomials on $\mathbb{R}$ both follow from the fact that $\mathbb{R}$ is a field. This proves the following.

Corollary 6. *For any field $\mathbb{F}$, polynomials are defined just as for $\mathbb{R}$. Furthermore both properties of Theorem 2 hold for polynomials on $\mathbb{F}$; and the Lagrange interpolation algorithm still interpolates any given $d+1$ points in $\mathbb{F}^2$ with a polynomial of degree at most d on $\mathbb{F}$.*

5. Secret Sharing

Recall from class the following application of Lagrange interpolation on $\mathbb{F}_m$. A GSI wishes to distribute secret $s \in \mathbb{Z}$ among n CS70 students $1,\ldots,n$ so that at least k of these students must get together in order to reconstruct s from each of their pieces of information.

Protocol 7. The secret sharing protocol:

i. The GSI and students agree on a prime $q > n, s$.

---

[1] Binary operators take two elements of $\mathbb{F}$ as input—think $+(a,b)$ or $a+b$ as the $+$ operator acting on points $a,b \in \mathbb{F}$.

[2] A non-prime integer.

ii. The GSI picks (in secret) any $k-1$ degree polynomial $P(x)$ on $\mathbb{F}_q$ such that $P(0) = s$.
iii. The GSI distributes $P(i)$ to student i, for each $1 \leq i \leq n$.
iv. Any group of k students can get together and construct the (at most) $k-1$ degree Lagrange polynomial $L(x)$ that fits their respective $P(i)$ values.
v. Property 2 ensures that $L = P$ and so that $L(0) = P(0) = s$.

Exercise 3. Suppose (!) you're a CS70 student, and your GSI has distributed a secret s to 10 students including yourself and your neighbor. The GSI picked a polynomial $P(x)$ of degree 2 (and so s/he hopes that no fewer than $k = 3$ students could reconstruct s) modular $q = 11$. Suppose the two of you are told that $P(6) \equiv 7 \mod 11$ and that $P(7) \equiv 5 \mod 11$. What can you say about s?

Exercise 4. What if you make friends with another student who tells you that $P(8) \equiv 7 \mod 11$? If possible, determine s.