CS 70 SPRING 2007 — DISCUSSION #5

ALEX FABRIKANT

1. Administrivia

(1) Course Information
- Next homework is **due February 20th** at 2:30pm in 283 Soda Hall; please put your section time on your homework.
- This Monday, 02/19, is a holiday (President's Day). Instead of my normal office hours, I will hold office hours **Monday 10pm-11pm at the Cafe Milano**[1]. I may be there as early as 9pm, but no promises.
- Homework 2 stats: mean 20.8/23, standard deviation 4.5, median 22.5
- Midterm 1 will be on Tuesday, March 6th, in class. All exam dates are now posted on the course website.

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 3. Find (and prove) an upper-bound on the number of times two different 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 4. 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: February 15, 2007.

The author gratefully acknowledges the TA's of CS70 Past for the use of their previous notes: Amir Kamil, Chris Crutchfield, David Garmire, Lorenzo Orecchia, and Ben Rubinstein. Their notes form the basis for this handout.

[1] 2532 Bancroft Ave, across Bancroft from Sproul Hall. **If Cafe Milano closes early**, I'll move to Cafe Strada, at the intersection of Bancroft&College.

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

Exercise 6. If I asked for a degree-3 polynomial that goes through some 4 distinct points $(a,0),(b,0),(c,0),(d,0)$, what would Lagrange interpolation produce? Why?

4. Secret Sharing

Recall from class the following application of Lagrange interpolation on $\mathbb{F}_m$. The government wishes to distribute the secret nuclear lunch code $s \in \mathbb{Z}$ among n generals $1,\ldots,n$ so that at least k of the generals must get together in order to reconstruct s from each of their pieces of information so as to nuke their country of choice.

Protocol 7. The secret sharing protocol:

i. The government picks a prime $q > n, s$ and announces it to the generals.
ii. The government picks (in secret) any $k-1$ degree polynomial $P(x)$ on $\mathbb{F}_q$ such that $P(0) = s$.
iii. The government distributes $P(i)$ to each general i, for each $1 \le i \le n$.
iv. Any group of k generals 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 8. Suppose the secret number is $s = 5$, there are $n = 3$ generals, and we want any 2 of them to be able to discover the secret.

(1) Pick some appropriate prime q and polynomial P over $\mathbb{F}_q$.
(2) Find the 3 values to hand out to the generals.
(3) Check that generals 1 and 2 can discover s.

Exercise 9. A Stanford student asks, "Why bother with this whole polynomial mess? For the problem above, why don't you just write your secret as a 3-digit binary number (101), tell the generals that the secret is some binary number between 000 (0) and 111 (7), and then give bits 1&2 to general 1, bits 1&3 to general 2, and bits 2&3 to general 3? That way, none of them will know the code without talking to at least one other general." Why is this approach worse?

5. Fancier secret-sharing

This mechanism can be used for more fancy secret-sharing setups.

Exercise 10. After a revolution, the new government decides to be more careful about sharing nuclear codes. Now, in order to obtain the code, we want to require at least 3 of (i) the Senate, (ii) the House, (iii) the Cabinet, and (iv) the Secret Cabal Of Soda Hall to participate. Furthermore, each one of those 4 bodies consists of 6 or more people, and in order for the body to participate, at least 3 of those people must be involved.

(1) How can we use the basic mechanism to set this up?
(2) Split yourselves up into 4 groups of 6 (or more) and let's try to put together the code. Your share of the secret will be handed out shortly.
(3) One night, the Secret Cabal of Soda Hall breaks into the fileserver storing the current constitution, and changes the constitution so that, if the Cabal participates, only *one* other body's participation is needed to obtain the full code. How can this be arranged without altering the other rules?

6. Challenge problem (a bit easier than usual)

Exercise 11. While we've shown at class that a degree-d polynomial over $\mathbb{F}_p$ has *at most* d roots, we didn't claim there are always d roots. Show that, for all primes p, there's a non-constant polynomial over $\mathbb{F}_p$ which has no roots. Given a p, what is the lowest degree d such that there exists a zero-less polynomial of degree d?

7. For your reference only: formal definition of fields (e.g. $\mathbb{F}_m$)

I'm including this section in case you're interested in the formal details of what it takes for something to be a field. This is **not part** of what we expect you to learn in CS70. For a lot more interesting details about fields, take Math 113 (Abstract Algebra).

Definition 12. Let $\mathbb{F}$ be a set endowed with binary operators[2] $+$ 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 13. 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[3] 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 14. *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 $\mathbb{F}$.*

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

[3] A non-prime integer.