CS 70 Fall 2016 | Discrete Mathematics and Probability Theory Seshia and Walrand | HW 6

1. **Sundry**

   Before you start your homework, write down your team. Who else did you work with on this homework? List names and email addresses. (In case of hw party, you can also just describe the group.) How did you work on this homework? Working in groups of 3-5 will earn credit for your "Sundry" grade.

   Please copy the following statement and sign next to it:

   I certify that all solutions are entirely in my words and that I have not looked at another student's solutions. I have credited all external sources in this write up.

2. $d+2$ **points vs. a polynomial of degree** d

   (a) Given 3 points $(0,1)$, $(1,1)$, and $(2,3)$, use Lagrange interpolation to construct the degree-2 polynomial which goes through these points.

   (b) Given 4 points $(0,1)$, $(1,1)$, $(2,3)$, and $(-1,3)$, does there exist a degree-2 polynomial which goes through these points? If yes, find the polynomial; if no, explain why none exists.

   (c) Given 4 points $(0,1)$, $(1,1)$, $(2,3)$, and $(-1,0)$, does there exist a degree-2 polynomial which goes through these points? If yes, find the polynomial; if no, explain why none exists.

   (d) Design a machine (i.e. give the pseudocode for an algorithm) with the following function: given four points $(x_1,y_1),(x_2,y_2),(x_3,y_3),(x_4,y_4)$ with all the x_i distinct, the machine outputs YES if there exists a polynomial $p(x)$ of degree at most 2 such that $p(x_i)=y_i$ for all i; otherwise, it outputs NO.

3. **(Proofs about polynomials)**

   In this problem, you will give two different proofs of the following theorem: For every prime p, every polynomial over $GF(p)$, even polynomials with degree $\geq p$, is equivalent to a polynomial of degree at most $p-1$. (Two polynomials f,g over $GF(p)$ are said to be equivalent iff $f(x)=g(x)$ for all $x \in GF(p)$.)

   (a) Show how the theorem follows from Fermat's Little Theorem.

   (b) Now prove the theorem using properties of polynomials.

4. **GCD of Polynomials**

   Let $A(x)$ and $B(x)$ be polynomials (with coefficients in $\mathbb{R}$ or $GF(m)$). We say that $\gcd(A(x),B(x)) = D(x)$ if $D(x)$ divides $A(x)$ and $B(x)$, and if every polynomial $C(x)$ that divides both $A(x)$ and

$B(x)$ also divides $D(x)$. For example, $\gcd((x-1)(x+1),(x-1)(x+2)) = x-1$. Incidentally, $\gcd(A(x),B(x))$ is the highest degree polynomial that divides both $A(x)$ and $B(x)$.

(a) Write a recursive program to compute $gcd(A(x),B(x))$. You may assume you already have a subroutine for dividing two polynomials.

(b) Let $P(x) = x^4 - 1$ and $Q(x) = x^3 + x^2$ in standard form. Prove there are no polynomials $A(x)$ and $B(x)$ such that $A(x)P(x) + B(x)Q(x) = 1$ for all x.

(c) Find polynomials $A(x)$ and $B(x)$ such that $A(x)P(x) + B(x)Q(x) = x+1$ for all x.

5. **Properties of** $GF(p)$

(a) Show that, if $p(x)$ and $q(x)$ are polynomials over the reals (or complex, or rationals) and $p(x) \cdot q(x) = 0$ for all x, then either $p(x) = 0$ for all x or $q(x) = 0$ for all x or both (*Hint*: You may want to prove first this lemma, true in all fields: The roots of $p(x) \cdot q(x)$ is the union of the roots of $p(x)$ and $q(x)$.)

(b) Show that the claim in part (a) is false for finite fields $GF(p)$.

6. **Erasures: Lagrange or Linear System**

Say we do the erasure coding scheme discussed in note 9, where a three packet message is sent using a polynomial $P(x)$, where $P(0) = m_1, P(1) = m_2$, and $P(2) = m_3$, and $P(3)$ and $P(4)$ are also sent. The channel loses $P(0)$ and $P(4)$.

In this exercise, we will try to find the polynomial $P(x)$ of degree at most 2 with coefficients in GF(5) such that $P(1) = 2 \pmod 5$, $P(2) = 4 \pmod 5$, and $P(3) = 3 \pmod 5$ and recover the original message.

(a) Find the $\Delta_i(x)$ polynomials for $i \in \{1,2,3\}$.

(b) Combine the Δ_is with the right coefficients to find the polynomial $P(x)$.

(c) Now we will try a different approach. Write the polynomial $P(x)$ as $c_0 + c_1x + c_2x^2$. Treating c_is as variables, what do the equations $P(1) = 2 \pmod 5$, $P(2) = 4 \pmod 5$, and $P(3) = 3 \pmod 5$ tell us about the c_is?

(d) Solve the system of equations you got from the last part to solve for the c_is. What is the resulting polynomial $P(x)$?

(e) What was the original message that was sent?

7. **Trust No One**

Gandalf has assembled a fellowship of eight people to transport the One Ring to the fires of Mount Doom: four hobbits, two men, one elf, and one dwarf. The ring has great power that may be of use to the fellowship during their long and dangerous journey. Unfortunately, the use of its immense power will eventually corrupt the user, so it must not be used except in the most dire of circumstances. To safeguard against this possibility, Gandalf wishes to keep the instructions a secret from members of the fellowship. The secret must only be revealed if enough members of the fellowship are present and agree to use it.

Requiring all eight members to agree is certainly a sufficient condition to know the instructions, but it seems excessive. However, we also know that the separate races (hobbits, men, elf, and dwarf) do not completely trust each other so instead we decide to require members from at least two races in order to use the ring. In particular, we will require a unanimous decision by all members of one race in addition to at least one member of a different race. That is, if only the four hobbits want to use the ring, then they alone should not have sufficient information to figure out the instructions. Same goes for the two men, the elf, and the dwarf.

More explicitly, some examples: only four hobbits agreeing to use the ring is not enough to know the instructions. Only two men agreeing is not enough. Only the elf agreeing is not enough. Only the dwarf agreeing is not enough. All four hobbits and a man agreeing is enough. Both men and a dwarf agreeing is enough. Both the elf and the dwarf agreeing is enough.

Gandalf has hired your services to help him come up with a secret sharing scheme that accomplishes this task, summarized by the following points:

- There is a party of four hobbits, two men, an elf, and a dwarf.
- There is a secret message that needs to be known if enough members of the party agree.
- The message must remain unknown to everyone (except Gandalf) if not enough members of the party agree.
- If only the members of one race agree, the message remains a secret.
- If all the members of one race agree plus at least one additional person, the message can be determined.
- Other combinations of members (e.g. two hobbits and a man) can either determine the message or keep it a secret (it is up to your discretion).