1 How Many Polynomials?

Let $P(x)$ be a polynomial of degree at most 2 over GF(5). As we saw in lecture, we need $d+1$ distinct points to determine a unique d-degree polynomial, so knowing the values for say, $P(0)$, $P(1)$, and $P(2)$ would be enough to recover P. (For this problem, we consider two polynomials to be distinct if they return different values for any input.)

(a) Assume that we know $P(0) = 1$, and $P(1) = 2$. Now consider $P(2)$. How many values can $P(2)$ have? How many distinct possibilities for P do we have?

(b) Now assume that we only know $P(0) = 1$. We consider $P(1)$ and $P(2)$. How many different $(P(1), P(2))$ pairs are there? How many distinct possibilities for P do we have?

(c) Now, let P be a polynomial of degree at most d. Assume we only know P evaluated at $k \leq d+1$ different values. How many different possibilities do we have for P?

Solution:

(a) 5 polynomials, each for different values of $P(2)$.

(b) Now there are 5^2 different polynomials.

(c) p^{d+1-k} different polynomials. For $k = d+1$, there should only be 1 polynomial.

2 Polynomial Practice

(a) If f and g are non-zero real polynomials, how many roots do the following polynomials have at least? How many can they have at most? (Your answer may depend on the degrees of f and g.)

   (i) (2 points) $f+g$

   (ii) (2 points) $f \cdot g$

   (iii) (2 points) f/g, assuming that f/g is a polynomial

(b) Now let f and g be polynomials over GF(p).

   (i) (3 points) We say a polynomial $f = 0$ if

$$\forall x, f(x) = 0$$

   . If $f \cdot g = 0$, is it true that either $f = 0$ or $g = 0$?

(ii) (3 points) If $\deg f \geq p$, show that there exists a polynomial h with $\deg h < p$ such that $f(x) = h(x)$ for all $x \in \{0, 1, ..., p-1\}$.

(iii) (3 points) How many f of degree *exactly* $d < p$ are there such that $f(0) = a$ for some fixed $a \in \{0, 1, \ldots, p-1\}$?

(c) (5 points) Find a polynomial f over GF(5) that satisfies $f(0) = 1, f(2) = 2, f(4) = 0$. How many such polynomials are there?

Solution:

(a) (i) It could be that $f+g$ has no roots at all (example: $f(x) = 2x^2 - 1$ and $g(x) = -x^2 + 2$), so the minimum number is 0. However, if the highest degree of $f+g$ is odd, then it has to cross the x-axis at least once, meaning that the minimum number of roots for odd degree polynomials is 1 (we did not look for this case when grading). On the other hand, $f+g$ is a polynomial of degree at most $m = \max(\deg f, \deg g)$, so it can have at most m roots. The one exception to this expression is if $f = -g$. In that case, $f+g = 0$, so the polynomial has an infinite number of roots!

(ii) A product is zero if and only if one of its factors vanishes. So if $f(x) \cdot g(x) = 0$ for some x, then either x is a root of f or it is a root of g, which gives a maximum of $\deg f + \deg g$ possibilities. Again, there may not be any roots if neither f nor g have any roots (example: $f(x) = g(x) = x^2 + 1$).

(iii) If f/g is a polynomial, then it must be of degree $d = \deg f - \deg g$ and so there are at most d roots. Once more, it may not have any roots, e.g. if $f(x) = g(x)(x^2+1)$, $f/g = x^2 + 1$ has no root.

(b) (i) **Example 1:** $x^{p-1} - 1$ and x are both non-zero polynomials on $GF(p)$ for any p. x has a root at 0, and by Little Fermat, $x^{p-1} - 1$ has a root at all non-zero points in $GF(p)$. So, their product $x^p - x$ must have a zero on all points in $GF(p)$.

Example 2: To satisfy $f \cdot g = 0$, all we need is $(\forall x \in S, f(x) = 0 \vee g(x) = 0)$ where $S = \{0, \ldots, p-1\}$. We may see that this is not equivalent to $(\forall x \in S, f(x) = 0)) \vee (\forall x \in S, g(x) = 0)$.

To construct a concrete example, let $p = 2$ and we enforce $f(0) = 1, f(1) = 0$ (e.g. $f(x) = 1 - x$), and $g(0) = 0, g(1) = 1$ (e.g. $g(x) = x$). Then $f \cdot g = 0$ but neither f nor g is the zero polynomial.

(ii) Little Fermat tells us that $x^s \equiv x \cdot x^{(s-1) \bmod (p-1)} \pmod p$ (note that we have to factor one x out to account for the possibility that $x = 0$), and since $(s-1) \bmod (p-1) \leq p-2$, writing $f(x) = \sum_{k=0}^{n} a_k x^k$, we have that $h(x) = a_0 + \sum_{k=1}^{n} a_k x \cdot x^{(k-1) \bmod (p-1)}$ is a polynomial of degree $\leq p-1$ with $f(x) = h(x)$.

(iii) We know that in general each of the $d+1$ coefficients of $f(x) = \sum_{k=0}^{d} c_k x^k$ can take any of p values. However, the conditions $f(0)$ and $\deg f = d$ impose constraints on the constant coefficient $f(0) = c_0 = a$ and the top coefficient $x_d \neq 0$. Hence we are left with $(p-1) \cdot p^{d-1}$ possibilities.

(c) We know by part (b) that any polynomial over GF(5) can be of degree at most 4. A polynomial of degree ≤ 4 is determined by 5 points (x_i, y_i). We have assigned three, which leaves $5^2 = 25$ possibilities. To find a specific polynomial, we use Lagrange interpolation:

$$\Delta_0(x) = 2(x-2)(x-4) \qquad \Delta_2(x) = x(x-4) \qquad \Delta_4(x) = 2x(x-2),$$

and so $f(x) = \Delta_0(x) + 2\Delta_2(x) = 4x^2 + 1$.

3 The CRT and Lagrange Interpolation

Let $n_1, \ldots n_k$ be pairwise coprime, i.e. n_i and n_j are coprime for all $i \neq j$. The Chinese Remainder Theorem (CRT) tells us that there exist solutions to the following system of congruences:

$$\begin{aligned}
x &\equiv a_1 \pmod{n_1} && (1)\\
x &\equiv a_2 \pmod{n_2} && (2)\\
&\vdots && (\vdots)\\
x &\equiv a_k \pmod{n_k} && (k)
\end{aligned}$$

and all solutions are equivalent $\pmod{n_1 n_2 \cdots n_k}$. For this problem, parts (a)-(c) will walk us through a proof of the Chinese Remainder Theorem. We will then use the CRT to revisit Lagrange interpolation.

(a) We start by proving the $k = 2$ case: Prove that we can always find an integer x_1 that solves (1) and (2) with $a_1 = 1, a_2 = 0$. Similarly, prove that we can always find an integer x_2 that solves (1) and (2) with $a_1 = 0, a_2 = 1$.

(b) Use part (a) to prove that we can always find at least one solution to (1) and (2) for any a_1, a_2. Furthermore, prove that all possible solutions are equivalent $\pmod{n_1 n_2}$.

(c) Now we can tackle the case of arbitrary k: Use part (b) to prove that there exists a solution x to (1)-(k) and that this solution is unique $\pmod{n_1 n_2 \cdots n_k}$.

(d) For two polynomials $p(x)$ and $q(x)$, mimic the definition of $a \bmod b$ for integers to define $p(x) \bmod q(x)$. Use your definition to find $p(x) \bmod (x-1)$.

(e) Define the polynomials $x - a$ and $x - b$ to be coprime if they have no common divisor of degree 1. Assuming that the CRT still holds when replacing x, a_i and n_i with polynomials (using the definition of coprime polynomials just given), show that the system of congruences

$$\begin{aligned}
p(x) &\equiv y_1 \pmod{(x-x_1)} && (1')\\
p(x) &\equiv y_2 \pmod{(x-x_2)} && (2')\\
&\vdots && (\vdots)\\
p(x) &\equiv y_k \pmod{(x-x_k)} && (k')
\end{aligned}$$

has a unique solution $\pmod{(x-x_1)\cdots(x-x_k)}$ whenever the x_i are pairwise distinct. What is the connection to Lagrange interpolation?

Solution:

(a) Since $\gcd(n_1, n_2) = 1$, there exist integers k_1, k_2 such that $1 = k_1 n_1 + k_2 n_2$. Setting $x_1 = k_2 n_2 = 1 - k_1 n_1$ and $x_2 = k_1 n_1 = 1 - k_2 n_2$ we obtain the two desired solutions.

(b) Using the x_1 and x_2 we found in Part (a), we show that $a_1 x_1 + a_2 x_2 \pmod{n_1 n_2}$ is a solution to the desired equivalences:

$$\begin{aligned} a_1 x_1 + a_2 x_2 &\equiv a_1 \cdot 1 + a_2 \cdot 0 \equiv a_1 \pmod{n_1} \\ a_1 x_1 + a_2 x_2 &\equiv a_1 \cdot 0 + a_2 \cdot 1 \equiv a_2 \pmod{n_2}. \end{aligned}$$

Such result is also unique. Say that we have two difference solutions $x = c$ and $x = c'$, which both satisfy $x \equiv a_1 \pmod{n_1}$ and $x \equiv a_2 \pmod{n_2}$. This would give us $c \equiv c' \pmod{n_1}$ and $c \equiv c' \pmod{n_2}$, which suggests that $(c - c')$ is divisible by n_1 and n_2. Since n_1 and n_2 are coprime, $gcd(n_1, n_2) = 1$, $(c - c')$ is divisible by $n_1 n_2$. Writing it in modular form gives us $c \equiv c' \pmod{n_1 n_2}$. Therefore, all the result is unique with respect to $\pmod{n_1 n_2}$

(c) We use induction on k. Part (b) handles the base case, $k = 2$. For the inductive hypothesis, assume for $k \leq l$, the system (1)-(k) has a unique solution $a \pmod{n_1 \cdots n_k}$. Now consider $k = l + 1$, so we add the equation $x \equiv a_{l+1} \pmod{n_{l+1}}$ to our system, resulting in

$$\begin{aligned} x &\equiv a \pmod{n_1 \cdots n_l} \\ x &\equiv a_{l+1} \pmod{n_{l+1}}. \end{aligned}$$

Since the n_i are pairwise coprime, $n_1 n_2 \cdots n_l$ and n_{l+1} are coprime. Part (b) tells us that there exists a unique solution $a' \pmod{n_1 \cdots n_l n_{l+1}}$. We conclude that a' is the unique solution to (1)-($l+1$), when taken $\pmod{n_1 n_2 \cdots n_l n_{l+1}}$.

(d) a mod b is defined as the remainder after division by b. But we know how to divide polynomials and compute remainders too! In particular, we know that we can write $p(x) = q'(x)q(x) + r(x)$ where $\deg r < \deg q$. So we define $p(x) \bmod q(x) = r(x)$.

To compute $p(x) \bmod (x-1)$ then, we write $p(x) = (x-1)q'(x) + r(x)$. We know that $\deg r < \deg(x-1) = 1$ and so r must be a constant. Which constant is it? Plugging in $x = 1$ gives $p(1) = r(1)$ and so $r(x) = p(1)$ for all x.

(e) We only need to check that $q_i(x) = (x - x_i)$ and $q_j(x) = (x - x_j)$ are coprime whenever $x_i \neq x_j$; that is, that they don't share a common divisor of degree 1. If $d_i(x) = a_i x + b_i$ is a divisor of $q_i(x)$, then $q_i(x) = q'(x)(a_i x + b_i)$ for some polynomial $q'(x)$. But since $q_i(x)$ is of degree 1, $q'(x)$ must be of degree 0 and hence a constant, so $d_i(x)$ must be a constant multiple of $q_i(x)$. Similarly, any degree 1 divisor d_j of $q_j(x)$ must be a constant multiple of $q_j(x)$, and if $x_i \neq x_j$, then none of these multiples overlap, so $q_i(x)$ and $q_j(x)$ are coprime.

From our result in part (d), the congruences ($1'$)-(k') assert that we are looking for a polynomial $p(x)$ such that $p(x_i) = y_i$. The CRT then establishes the existence of $p(x)$, and that it is unique modulo a degree k polynomial. That is, $p(x)$ is unique if its degree is at most $k - 1$. Lagrange interpolation finds $p(x)$.