CS70 HW 6

Mar 6, 2021

1 Polynomial Practice

(a) Say function f degree is d_f, function g is d_g.

(i) at least 0, at most $max\{d_f, d_g\}$. Because $0 \leq degree(f+g) \leq max\{d_f, d_g\}$.

(ii) at least 0, at most $d_f + d_g$. Because $0 \leq degree(f \cdot g) \leq d_f + d_g$.

(iii) at least 0, at most $d_f - d_g$. Because $0 \leq degree(f/g) \leq d_f - d_g$.

(b) (i) $0 \leq degree(f \cdot g) \leq d_f + d_g$. Therefore, $d_f + d_g = 0 \implies d_f = 0 \vee d_g = 0$. Thus either $f = 0$ or $g = 0$.

Didn't see the GF(p) in the question.

we can construct $f(x) = x^{p-1} - 1$ and $g(x) = x$, in which $f(x) \equiv 0 \pmod p$ except $x = 0$, and $g(x) \equiv 0 \pmod p$ when $x = 0$, thus $f \cdot g \equiv 0 \pmod p$ in all range.

Or proof by contradiction.

Proof. Say $f \neq 0 \wedge g \neq 0$, then $f * g \neq 0$, which contradicts to $f * g = 0$. $\square$

(ii) By Fermat's little theorem, for any $x \in \{0, 1, \ldots, p-1\}, x^{p-1} \equiv 1 \pmod p) if GF(p)$. Any degree $y \geq p$ can be expressed $x^y \equiv x^a \pmod p$ where $a \in \{0, 1, \ldots, p-1\}$.

(iii) d degree needs $d+1$ points to interpolate.
now (0, a) is fixed $\implies$ needs d points.
All points have p choices $\implies$ p^d number of polynomials.

(c) Given three points, we can def $p(x) = ax^2 + bx + c$ and have equations:

$$
\begin{aligned}
c &= 1 \\
4a + 2b + c &= 2 \\
16a + 4b + c &= 0
\end{aligned}
$$

Solving there equations, we have $c = 1, a = -3/8, b = 5/4$. Therefore, $g(x) = \frac{-3}{8}x^2 + \frac{5}{4}x + 1$.
And for polynomials that degree is greater than 2, there are 5 choices for degree 3, $5^2 = 25$ choices for degree 4.
Thus in total : 31 polynomials.

in total:25. The degree 4 situation includes degree 3.

2 The CRT and Lagrange Interpolation

(a) Since $a_2 = 0$, so x is multiple of n_2, aka $x = kn_2$. But from $x \equiv a_1 \pmod{n_1}$ and $x * x^{-1} \equiv 1 \pmod{n_1}$, we can construct $x_1 = kn_2 * (kn_2)^{-1} = n_2 * (n_2)^{-1} \pmod{n_1}$. Similarly, for $a_1 = 0, a_2 = 1$, we can construct $x_2 = n_1 * (n_1)^{-1} \pmod{n_2}$.

(b) For any a and b, we can use the solution from part (a), to obtain $X = ax_1 + bx_2$. Therefore, there is at least one solution.

For uniqueness, take $x_1 = n_2 * (n_2)^{-1} \pmod{n_1}$ for example, since $gcd(n_1, n_2) = 1$, so the $(n_2)^{-1}$ is unique and make x_1 is unique $\pmod{n_1}$ also. x_2 is unique as the same reason.

(c) *Proof.* Proof by Induction on the number of the equation k.

Base Case: When $k = 1, x \equiv a_1 \pmod{n_1}$, obviously x exists and is unique.

Induction Hypothese: Assume when $k = m$, the equation holds and the result $x_m \equiv a_m \pmod{n_m}$.

Induction Step: Use the part b, we know there is a unique solution of the equation

$$\begin{aligned} x_m &\equiv a_m \pmod{n_m} \\ x_{m+1} &\equiv a_{m+1} \pmod{n_{m+1}} \end{aligned}$$

so proof is done.

$\square$

(d) For integer $a, b, a = b * Q + R$ and $a \equiv R \pmod{q}$.
To mimic such relation, $P(x) = q(x) * Q(x) + R(x)$ and $P(x) \equiv R(x) \pmod{q(x)}$.

To compute $p(x) \bmod (x-1)$, say $p(x) = a_0 + a_1 x + \cdots + a_k x^k$. For x^n, we can express it as $((x-1)+1)^n$, which is $\equiv 1 \pmod{x-1}$. So $p(x) \equiv \sum_{i=0}^{k} a_i \pmod{x-1}$.

(e) Given CRT still holds when replacing x, a_i and n_i with polynomials, now we just need to prove that $(x - x_i)$ are coprime when x_i are pairwise distinct.

Proof. Proof by contradiction.
Say $(x - x_i)$ and $(x - x_k)$ are not coprime when $x_i \neq x_k$. By the definition of coprime in polynomial, there is a degree 1 polynomial, i.e $(x - a)$ dividing both. Since $(x - x_i)$ is degree 1, if it's divided by $(x - a)$, a must be x_i. It's also same when $(x - x_k)$, so a must be x_k. So $x_i = x_k$, which contradicts to $x_i \neq x_k$. So $(x - x_i)$ are coprime. □

The relation with Lagrange interpolation: the solution is exactly the way of Lagrange interpolation construction. Since in points interpolation, x_i are pairwise distinct, so the solution is consistent and unique.

3 Old secrets, new secrets

The answer is simple, joke on his information of $(1, P(1))$, say give his friends $(1, P(1)')$ where $P(1)' \neq P(1)$. Since there is unique polynomial each with n points with $(1, P(1))$ and $(1, P(1)')$, the former one will get original secret s, while the latter one will get s' where $s' \neq s$.

4 Berlekamp-Welch for General Errors

(a) Degree of E(x): 1;
Degree of Q(x): 3;
$E(x) = x - b.Q(x) = a_0 + a_1x + a_2x^2 + a_3x^3$. And have the equation:

$$\begin{aligned}
a_0 + -3(-b) &= 0 \\
a_0 + a_1 + a_2 + a_3 - 7(1 - b) &= 0 \\
a_0 + 2a_1 + 4a_2 + 8a_3 - 0(2 - b) &= 0 \\
a_0 + 3a_1 + 9a_2 + 27a_3 - 2(3 - b) &= 0 \\
a_0 + 4a_1 + 16a_2 + 64a_3 - 10(4 - b) &= 0
\end{aligned}$$

(b) Solving the equation, we have $(a_0, a_1, a_2, a_3, b) = (8, 5, 6, 3, 1)$; So $Q(x) = 8 + 5x + 6x^2 + 3x^3$, $E(x) = x - 1$. So the first message is wrong.

(c) $P(x) = Q(x)/E(x) = 3x^2 + 9x + 3$. So $P(1) = 15 \equiv 4 \pmod{11}.P(1) = E$. Original message DEACK.

5 Error-Detecting Codes

Since it's detecting not correcting, the number of symbols needed is $n+1$, aka one more symbol to tell if there is an error occurring. There are two cases:

(i) No error. Then the polynomial interpolated by the first n symbols is consistent on the $(n+1)$th point.

(ii) There are errors. Then the $(n+1)$th point is inconsistent on the polynomial no matter how many errors occurs.

Now we show that any number lesser n + 1 is not gonna work. Say, we send n symbols, then we don't know whether errors had occurred since there is only one polynomial. Any symbol lesser n is impossible since there are n symbol needed to send.

Solution: Here I just consider when it loses only one symbol, thus making answer be n + 1. But when errors is greater than 1, it can construct a counter example, which leads the (n+1)th point is also consistent on the polynomial interpolated by the first n symbols.
Thus the correct answer is $n+k$. Still consider the polynomial interpolated by the first n symbols, aka$(x_1, P(x_1)), \ldots, (x_n, P(x_n))$ and also sends extra k points, from $n+1$ to $n+k$. Now we prove by cases:

(i) If there are no errors, then the points from $n+1$ to $n+k$ are all consistent by the h polynomial. h polynomials are interpolated by the received first n points.

(ii) If there is an error, we prove that there are some points in the range $(n+1, n+k)$ inconsistent. If these K error are all in the $(n+1, n+k)$, then it's obviously true. In other case, if some errors occur in the range $(1, n)$, meaning there are some true uncorrupted in the range $(n+1, n+k)$, thus h polynomial won't agree on that true point.

And for any number lesser than n + k, the reason is same as the mistake I made. There is still possibility that all points are consistent using the error points.