CS70 In Simpler Terms - Note 11

written by Kevin Liu cs70.kevinmliu.com

August 2, 2017

1 Error Correcting Codes

Suppose you are trying to send a message of n packets. There are two cases:

- Erasure code: k packets are erased, so you need at least $n + k$ packets
- General error: k packets are corrupted, so you need at least $n+2k$ packets
  This can be thought about intuitively in that if there are k corrupt packets, then you are left with $2k$ good packets, and the $2k$ good packets match up so you are more confident with your decision on which packets are corrupt
  Suppose you are trying to reconstruct $P(x)$ from the $(n + 2k)^+$ packets
  - (good) $P(i) = r(i)$ (received) for at least $n + k$ packets
  - let $E(x) = (x - e_1)...(x - e_k)$, where e_i = a corrupted packet, and there are k of those
  - $P(i)E(i) = r_iE(i)$ for $1 \leqslant i \leqslant n + 2k$ (all packets)
    since $P(i) = r_i$ for good packets and $E(i) = 0$ for corrupt packets
  - We now need to show that this is solvable:
    * Let $Q(x) = P(x)E(x)$, then $P(x) = \frac{Q(x)}{E(x)}$
    * $P(x)$ is of degree $n - 1$ (*n packets are necessary to construct an $n-1$ degree polynomial*), $E(x)$ is of degree k, so $Q(x)$ is of degree $n + k - 1$,
    * $Q(x) = a_{n+k-1}x^{n+k-1} + ...a_1x + a_0$ and there are $n+k$ unknown coefficients
    * $E(x) = 1x^k + (b_{k-1}x^{k-1} + ...b_1x + b_0)$ and there are k unknown coefficients
    * There are a total of $n + 2k$ unknown coefficients, and since we have $n + 2k$ total packets, we can contruct $n + 2k$ equations, and when *the number of equations = number of variables*, it's solvable!
    * **Note:** If the question states that the polynomial is restricted to a finite field, remember to $\pmod q$ constantly, where q is the field you are working within
      Example:
      · let $E(x) = x + b_0$
      · if $k = 1, b_0 = 6$, and the field $q = 7$
        $\Rightarrow E(x) = (x + 6) \pmod 7 \equiv (x - 1) \pmod 7$, so $e_1 = 1$
        Your solution to $E(x) = x - 1$

2 Secret Sharing

Example:

- any group of k can reconstruct the polynomial, $P(x)$ to figure out the secret code (usually at $P(0)$)
- If the group is $k-1$ or fewer, then they can't construct the polynomial easily *it will later be shown that having a group of $k-1$ people gives you no more information about the secret code than being given no values at all.*
- Let q be a very large prime number $>> n, s$
- $P(x)$ is of degree $k-1$ and $P(0) =$ s (secret code)
- $P(x) = a_1x^n + a_2x^{n-1} + ...a_n + s$
- $P(1)$ is given to the first person, $P(2)$ is given to the second person, ... $P(n)$ is given to the nth person
- If there are only $k-1$ values, s can take on the values $\{0, 1, ...q-1\} = q$ values still (as described in the chart from the previous note). And since you are working over $\pmod q$, there were q possibilities to begin with! so you had no more information with $k-1$ values than with 0 values...

3 More Examples

- $P(x)$ degree 4, $Q(x)$ is degree 2. What is the maximum number of intersections of the two polynomials?
  - $P(x) - Q(x) = 0$ has at most 4 zeroes = 4 points of intersections
- Simplify (remove the denominator) for the following:
  $\frac{(x-4)(x-5)}{2} \pmod 7 \equiv (x-4)(x-5)(\frac{1 \pmod 7}{2 \pmod 7})$
  - $\frac{1 \pmod 7}{2 \pmod 7} \equiv \frac{8}{2} \pmod 7 \equiv 4 \pmod 7$ OR
  - $\frac{1 \pmod 7}{2 \pmod 7} = x \pmod 7 \Rightarrow 1 \equiv 2x \pmod 7 \Rightarrow 2^{-1} = 4 \equiv 4 \pmod 7$