CS 70 Discrete Mathematics and Probability Theory
Summer 2019 James Hulett and Elizabeth Yang

DIS 3C

1 Secrets in the United Nations

The United Nations (for the purposes of this question) consists of n countries, each having k representatives. A vault in the United Nations can be opened with a secret combination $s \in \mathbb{Z}$. The vault should only be opened in one of two situations. First, it can be opened if all n countries in the UN help. Second, it can be opened if at least m countries get together with the Secretary General of the UN.

(a) Propose a scheme that gives private information to the Secretary General and n countries so that s can only be recovered under either one of the two specified conditions.

(b) The General Assembly of the UN decides to add an extra level of security: in order for a country to help, all of the country's k representatives must agree. Propose a scheme that adds this new feature. The scheme should give private information to the Secretary General and to each representative of each country.

Solution:

(a) Create a polynomial of degree $n-1$ and give each country one point. Give the Secretary General $n-m$ points, so that if he collaborates with m countries, they will have $n-m+m=n$ points and can reconstruct the polynomial. Without the General, n countries can come together and also recover the polynomial. No combination of the General with fewer than m countries can recover the polynomial.

Alternatively, we can have two schemes, one for each condition. For the first condition: just one polynomial of degree $\leq n-1$ would do, where each country gets one point. The polynomial evaluated at 0 would give the secret. For the second condition: one polynomial is created of degree $m-1$ and a point is given to each country. Another polynomial of degree 1 is created, where one point is given to the secretary general and the second point can be constructed from the first polynomial if m or more of the countries come together. With these two points, we have a unique 1-degree polynomial, which could give the secret evaluated at 0.

(b) The scheme in part (a) remains the same, but instead of directly giving each country a point on the $n-1$ degree polynomial to open the vault, construct an additional polynomial for each country that will produce that point.

Each country's polynomial has degree $k-1$, and a point is given to each of the k representatives of the country. Thus, when they all get together they can produce a point for either of the schemes.

2 Berlekamp-Welch Warm Up

Let $P(i)$, a polynomial applied to the input i, be the original encoded polynomial before sent, and let r_i be the received info for the input i which may or may not be corrupted.

(a) When does $r_i = P(i)$? When does r_i not equal $P(i)$?

(b) If you want to send a length-n message, what should the degree of $P(x)$ be? Why?

(c) If there are at most k erasure errors, how many packets should you send? If there are at most k general errors, how many packets should you send? (We will see the reason for this later.) Now we will only consider general errors.

(d) What do the roots of the error polynomial $E(x)$ tell you? Does the receiver know the roots of $E(x)$? If there are at most k errors, what is the maximum degree of $E(x)$? Using the information about the degree of $P(x)$ and $E(x)$, what is the degree of $Q(x) = P(x)E(x)$?

(e) Why is the equation $Q(i) = P(i)E(i) = r_iE(i)$ always true? (Consider what happens when $P(i) = r_i$, and what happens when $P(i)$ does not equal r_i.)

(f) In the polynomials $Q(x)$ and $E(x)$, how many total unknown coefficients are there? (These are the variables you must solve for. Think about the degree of the polynomials.) When you receive packets, how many equations do you have? Do you have enough equations to solve for all of the unknowns? (Think about the answer to the earlier question - does it make sense now why we send as many packets as we do?)

(g) If you have $Q(x)$ and $E(x)$, how does one recover $P(x)$? If you know $P(x)$, how can you recover the original message?

Solution:

(a) The received packet is correct; the received packet is corrupted.

(b) P has degree at most $n-1$ since n points determine a degree $\leq n-1$ polynomial.

(c) $n+k$; $n+2k$.

(d) The locations of corrupted packets. No ($E(x)$ is a polynomial that the receiver needs to compute in order to obtain $P(x)$). k. The degree of Q is $(n-1)+(k) = n+k-1$.

(e) If $P(i) = r_i$, then $P(i)E(i) = r_iE(i)$. If $P(i) \neq r_i$, then $E(i) = 0$.

(f) $(n+k-1+1)+(k) = n+2k$ unknowns. There are $n+2k$ equations. Yes (if the actual number of errors is less than k, then there will be multiple solutions).

(g) $P(x) = Q(x)/E(x)$. Compute $P(i)$ for $1 \leq i \leq n$. Alternatively, since we know the error-locator polynomial $E(x)$, we can find its roots to figure out which packets were corrupted and then we only need to evaluate $P(x)$ at the locations of the errors.

3 Berlekamp-Welch for General Errors

Suppose that Hector wants to send you a length $n = 3$ message, m_0, m_1, m_2, with the possibility for $k = 1$ error. For all parts of this problem, we will work mod 11, so we can encode 11 letters as shown below:

A	B	C	D	E	F	G	H	I	J	K
0	1	2	3	4	5	6	7	8	9	10

Hector encodes the message by finding the degree ≤ 2 polynomial $P(x)$ that passes through $(0, m_0)$, $(1, m_1)$, and $(2, m_2)$, and then sends you the five packets $P(0), P(1), P(2), P(3), P(4)$ over a noisy channel. The message you receive is

$$\text{DHACK} \Rightarrow 3, 7, 0, 2, 10 = r_0, r_1, r_2, r_3, r_4$$

which could have up to 1 error.

(a) First, let's locate the error, using an error-locating polynomial $E(x)$. Let $Q(x) = P(x)E(x)$. Recall that

$$Q(i) = P(i)E(i) = r_i E(i), \quad \text{for} \quad 0 \leq i < n + 2k.$$

What is the degree of $E(x)$? What is the degree of $Q(x)$? Using the relation above, write out the form of $E(x)$ and $Q(x)$ in terms of the unknown coefficients, and then a system of equations to find both these polynomials.

(b) Solve for $Q(x)$ and $E(x)$. Where is the error located?

(c) Finally, what is $P(x)$? Use $P(x)$ to determine the original message that Hector wanted to send.

Solution:

(a) The degree of $E(x)$ will be 1, since there is at most 1 error. The degree of $Q(x)$ will be 3, since $P(x)$ is of degree 2. $E(x)$ will have the form $E(x) = x + e$, and $Q(x)$ will have the form $Q(x) = ax^3 + bx^2 + cx + d$. We can write out a system of equations to solve for these 5 variables:

$$\begin{aligned} d &= 3(0+e) \\ a+b+c+d &= 7(1+e) \\ 8a+4b+2c+d &= 0(2+e) \\ 27a+9b+3c+d &= 2(3+e) \\ 64a+16b+4c+d &= 10(4+e) \end{aligned}$$

Since we are working mod 11, this is equivalent to:

$$\begin{aligned} d &= 3e \\ a+b+c+d &= 7+7e \\ 8a+4b+2c+d &= 0 \\ 5a+9b+3c+d &= 6+2e \\ 9a+5b+4c+d &= 7+10e \end{aligned}$$

(b) Solving this system of linear equations we get

$$Q(x) = 3x^3 + 6x^2 + 5x + 8.$$

Plugging this into the first equation (for example), we see that:

$$d = 8 = 3e \quad \Rightarrow \quad e = 8 \cdot 4 = 32 \equiv 10 \bmod 11$$

This means that

$$E(x) = x + 10 \equiv x - 1 \pmod{11}.$$

Therefore, the error occurred at $x = 1$ (so the second number sent in this case).

(c) Using polynomial division, we divide $Q(x) = 3x^3 + 6x^2 + 5x + 8$ by $E(x) = x - 1$:

$$P(x) = 3x^2 + 9x + 3$$

Then, $P(1) = 3 + 9 + 3 = 15 \equiv 4 \bmod 11$. This means that our original message was

$$3, 4, 0 \quad \Rightarrow \quad \text{DEA}.$$

Note: In Season 4 of Breaking Bad, Hector Salamanca (who cannot speak), uses a bell to spell out "DEA" (Drug Enforcement Agency).