CS 70 Discrete Mathematics and Probability Theory Fall 2021 Course Notes

DIS 5B

1 Berlekamp-Welch Warm Up

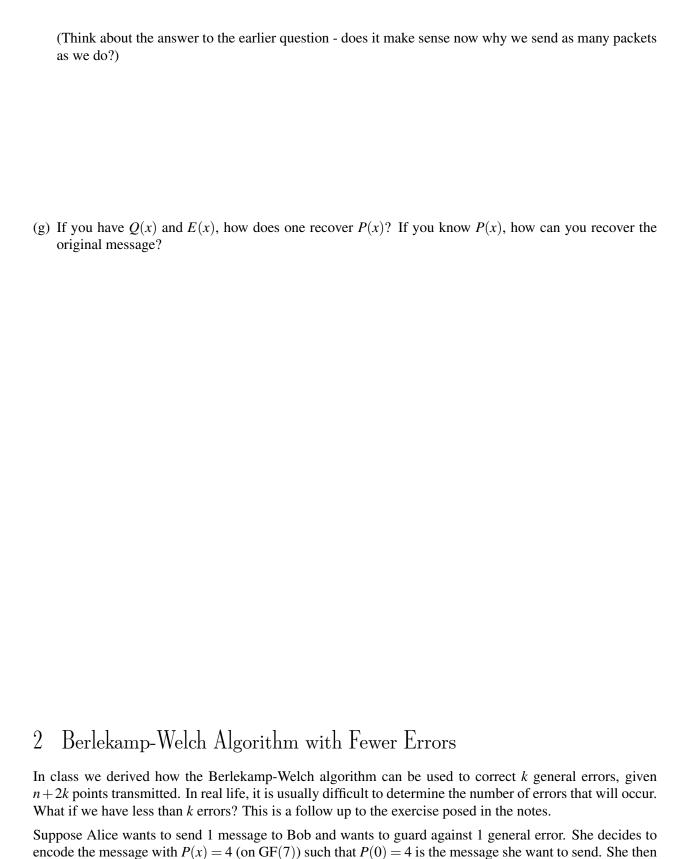
Let P(i), a polynomial applied to the input i, be the original encoded polynomial before sent, and let r_i be the received info for the input i which may or may not be corrupted.

- (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) represent? 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 .)

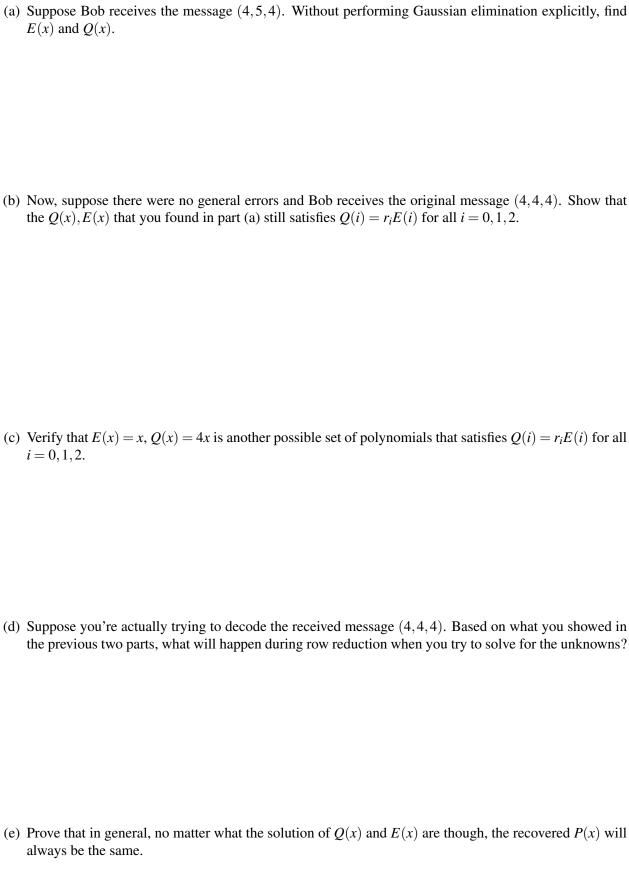
(f) In the polynomials Q(x) and E(x), how many total unknown coefficients are there? (These are the variables you must solve for. Think about the degree of the polynomials.) When you receive packets, how many equations do you have? Do you have enough equations to solve for all of the unknowns?

CS 70, Fall 2021, DIS 5B



CS 70, Fall 2021, DIS 5B 2

sends P(0), P(1), P(2) = (4, 4, 4) to Bob.



CS 70, Fall 2021, DIS 5B 3

3 Secret Sharing with Spies

An officer stored an important letter in her safe. In case she becomes unreachable in battle, she decides to share the password (which is a number) with her troops. However, everyone knows that there are 3 spies among the troops, but no one knows who they are except for the three spies themselves. The 3 spies can coordinate with each other and they will either lie and make people not able to open the safe, or will open the safe themselves if they can. Therefore, the officer would like a scheme to share the password that satisfies the following conditions:

- When *M* of them get together, they are guaranteed to be able to open the safe even if they have spies among them.
- The 3 spies must not be able to open the safe all by themselves.

Please help the officer to design a scheme to share her password. What is the scheme? What is the smallest *M*? Show your work and argue why your scheme works and any smaller *M* couldn't work. (The troops only have one chance to open the safe; if they fail the safe will self-destruct.)

CS 70, Fall 2021, DIS 5B 4