6 Secret Sharing, Berlekamp-Welch

Computer Science Mentors 70

March 9 - March 13
Spring 2020

Prepared by: Debayan Bandyopadhyay, Catherine Huang, Abinav Routhu, Robert Wang, Sebastien Whetsel
Reminder: This worksheet is not meant to be covered in two hours.
Feedback form: *tinyurl.com/csmcs70*

1 Splendid Secret-Sharing Schemes

1. (Discussion 4B Q3 points) The United Nations (for the purposes of this question) consists of n countries. A vault in the United Nations can be opened with a secret combination s. 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.

   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.

2. (Discussion 5A Q2 points) Suppose the Oral Exam questions are created by 2 TAs and 3 Readers. The answers are all encrypted and we know that:

   (a) Together, both TAs should be able to access the answers

   (b) All 3 Readers can also access the answers

   (c) One TA and one Reader should also be able to do the same

   Design a secret sharing scheme to make this work.

2 Mechanical Berlekamp-Welch

1. (Summer 19 HW5 Q3 points) In this question, we wish to send the message $(c_0, c_1, c_2) = (2, 3, 4)$ of length n = 3 through a channel that corrupts at most 1 packet. We will do arithmetic over GF(5).

   (a) Construct a polynomial $P(x) \pmod{5}$ of degree at most 2, so that $P(0) = 2$, $P(1) = 3$, $P(2) = 4$. What is the message $(c_0, c_1, c_2, c_3, c_4)$ that is sent? [The point of this is to get interpolation practice, even if the polynomial may be obvious]

(b) Suppose the message is corrupted by changing c_0 to 0. Set up the system of linear equations in the Berlekamp-Welch algorithm to find $Q(x)$, $E(x)$, and $P(x)$. [You do not need to solve the equations]

3 Covrup-ed Messqges

1. (HW6 Q2)In class we derived how the Berlekamp-Welch algorithm can be used to correct k general errors, given $n+2k$ points transmitted. In real life, it is usually difficult to determine the number of errors that will occur. What if we have less than k errors? This is a follow up to the exercise posed in the notes. Suppose Alice wants to send 1 message to Bob and wants to guard against 1 general error. She decides to encode the message with $P(x) = 4$ (on GF(7)) such that $P(0) = 4$ is the message she want to send. She then sends $P(0), P(1), P(2) = (4, 4, 4)$ to Bob.

(a) Suppose Bob receives the message $(4, 5, 4)$. Without performing Gaussian elimination explicitly, find $E(x)$ and $Q(x)$.

(b) Now, suppose there were no general errors and Bob receives the original message $(4, 4, 4)$. Show that the $Q(x)$, $E(x)$ that you found in part (a) still satisfies $Q(i) = r_i E(i)$ for all $i = 0, 1, 2$.

(c) Verify that $E(x) = x$, $Q(x) = 4x$ is another possible set of polynomials that satisfies $Q(i) = r_i E(i)$ for all $i = 0, 1, 2$.

(d) Suppose you're actually trying to decode the received message (4,4,4). Based on what you showed in the previous two parts, what will happen during row reduction when you try to solve for the unknowns?

(e) Prove that in general, no matter what the solution of $Q(x)$ and $E(x)$ are though, the recovered $P(x)$ will always be the same.

2. Suppose we want to send a message of length n packets, and we know $p = 20\%$ of the packets will be erased. How many extra packets should we send to ensure our message is received? What happens if p increases (say to 90%)? As a bonus, derive a general expression for how many packets you should send to transmit a message of length $n$over a channel that erases a constant fraction p of packets sent. [Note: this is more similar to how erasures and corruptions work in the real world]

3. Suppose we want to send a message of length n packets, and we know $p = 20\%$ of the packets will be corrupted. How many extra packets should we send to ensure our original message is received? What is the maximum p can be to ensure your message can be received?