Discussion 5B Recap

Tyler Zhu

March 13, 2020

1 Berlekamp-Welch

For error correction in the case of corruptions, we have the Berlekamp-Welch algorithm which allows one to recover any message of length n by sending $2k$ extra packets. Here's how.

1. Define $E(x) = (x - e_1) \dots (x - e_k)$ where e_i are the locations of the errors, and let $Q(x) = P(x)E(x)$.
2. Notice that $Q(i) = r_i E(i)$ for all transmitted i, i.e. $1 \leq i \leq n + 2k$. Since we have $n + 2k$ packets and there are $n + 2k$ unknowns (k from E, $n + k$ from Q), we can solve this linear system for $Q(x)$ and $E(x)$.
3. Finally, $P(x) = Q(x)/E(x)$ by polynomial long division.

There's a few intricacies here, like what if the number of errors is actually less than k (in which case, we can interpret e_i as being a trivial error) or how we know that such a solution is unique. The first problem of the discussion worksheet walks through all of this intuition in good detail, so I highly recommend that.