# CS70 Disc 06A

March 1, 2021

## 1 Berlekamp-Welch Warm Up

(a) If we use $x_i$ denotes roots of $E(x)$, when $n = x_i$, then $r_i \neq P(i)$; otherwise, when $n \neq x_i$, then $r_i = P(i)$.

(b) If the message has n pieces of message to send, the degree of P(x) should be n - 1.

Because there is a unique polynomial of degree n - 1 given n pairs of points.

(If the message itself has n length, the degree of polynomial is not constrained.)

(c) there are at most k erasure errors $\implies$ n + k packets should be sent.

there are at most k general errors $\implies$ n + 2k packets should be sent.

(d) Roots of the error polynomial E(x) tell the location of the error.

Receiver does know the roots of E(x) if properly using extra information.

Maximum degree of E(x) is K.

The degree of Q(x) = P(x)E(x) = n - 1 + K.

(e) To prove $Q(i) = P(i)E(i) = r_iE(i)$ is always true. There are two cases:

(1) When $P(i) = r_i$, where $E(i) \neq 0$, so multiply each side with E(i), $Q(i) = P(i)E(i) = r_iE(i)$ equation holds.

(2) When $P(i) \neq r_i$, where $E(i) = 0$, so $P(x)E(x) = 0, r_iE(i) = 0$, so $Q(i) = P(i)E(i) = r_iE(i)$ equation holds.

(f) Degree of Q(x) is n - 1 + K, unknown coefficient is n + K. Degree of E(x) is K, but one coefficient is fixed, therefore unknown coefficient is K. The total number of unknown is n + 2K.

The total equations received are n + 2K.

Yes, n + 2k equations for n + 2k unknown.

(g) Since we define $Q(x) = E(x)P(x)$, $P(x) = Q(x)/E(x)$. Now we know $P(x)$, the original message is $P(1), P(2), \ldots, P(n)$.

## 2 Berlekamp-Welch Algorithm

(a) Say $P(x) = ax^2 + bx + c$, we obtain the equation

$$\begin{aligned} c &= 4 \\ a + b + c &= 3 \\ 4a + 2b + c &= 2 \end{aligned}$$

Therefore, we can solve the equations to obtain $a = 0, b = 4, c = 4$; therefore, $P(x) = 4x + 4$. Message $(c_0, c_1, c_2, c_3, c_4) = (4, 3, 2, 1, 0)$.

(b) The message we receive $R = \{0, 3, 2, 1, 0)$. By the equation $Q(x) = P(x)E(x) = r_i E(x)$, def $Q(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3, E(x) = x - b$ we have

$$\begin{aligned} a_0 - 0 * (0 - b) &= 0 \\ a_0 + a_1 + a_2 + a_3 - 3(1 - b) &= 0 \\ a_0 + 2a_1 + 4a_2 + 8a_3 - 2(2 - b) &= 0 \\ a_0 + 3a_1 + 9a_2 + 27a_3 - 1(3 - b) &= 0 \\ a_0 + 4a_1 + 16a_2 + 64a_3 - 0(4 - b) &= 0 \end{aligned}$$

(c) Since $Q(x) = -x^2 + 4x$ and $E(x) = x$, we obtain $P(x) = Q(x)/E(x) = -x + 4 \pmod 5$, the original message $(m_1, m_2, m_3) = (4, 3, 2)$.

## 3 Bijections

(a) If the domain and range of f are N, then for $x = 0, f(x) = 0$; for $x \geq 1, f(x) = x$, so it's bijective.

(b) Since part(a) has proved the situation when the domain and range of f are N, we just need to see when $x \leq 0$ and $x \in Z$, when $x = -1, f(-1) = 1; x \leq -2, f(x) = 2x + 3$; Since $f(-1) = f(1)$ and the slope of $2x + 3$ is not 1. So it's not injective or surjective.

(c) Not injective, since $f(-1) = f(1)$;
Not surjective, for $y \in (-1, 0)$, there is no $x \in R$ that $f(x) = y$;
Surjective, for $y \in R$, there is $x \in R$ that $f(x) = y$;

## 4 Count It!

(a) N, the set of all natural numbers : countably infinite.

By the definition of countably infinite, N is countably infinite.

(b) Z, the set of all integers : countably infinite.

View Z as the combination of two sets, $A = N, B = \{x \mid x < 0 \wedge x \in Z\}$, we can enumerate the set A and B crossingly as the order $(0, -1, 1, -2, 2 \ldots)$;

(c) Q, the set of all rational numbers : countably infinite.

Since $Q \subseteq Z^2$ since any element $q$ of $Q$ can be represented as $q = \frac{z_1}{z_2}$. And since $Z^2$ can be enumerated by the spiral way in the note, so $Q$ is also countable.

(d) R, the set of all real numbers : uncountably infinite.

Since by the principle of Diagonalization, we can generate a $r$ from the listing of elements $\in R$ that $\notin$ all the listing of elements.

(e) The integers which divide 8 : countably infinite.

It's subset of integers $Z$;

(f) The integers which 8 divides : finite.

We can list all of them, [-8, -4, -2, -1, 1, 0, 1, 2, 4, 8].

(g) The functions from N to N : uncountably infinite.

Proof by Diagonalization and contradiction.

*Proof.* Assume the functions from N to N are countably infinite and listing all of them. Say first line of $f_1$ is the outputs of the integer from 0 to $\infty$ and etc. From Diagonalization, construct a map T that if $P_i(i)$ on the list is not 7, T(i) = 7; if $P_i(i)$ does equal to 7, put T(i) = 6;

$$T(i) = \begin{cases} 7 & p_i(i) \neq 7 \\ 6 & p_i(i) = 7 \end{cases}$$

Then T is not on the list, while T is function from N to N, which is contradiction. □

(h) Computer programs that halt : countably infinite.

Since computer programs that halt are subsets of computer programs, and computer programs are just some finite string, which are countable.

We shall also prove that the programs are infinite. Just taking an example, the number of programs whose function are just print, which could print onece, twice, third …are infinite number.

(i) Numbers that are the roots of nonzero polynomials with integer coefficients : finite.

For a polynomial of degree n, there are at most n roots.

Numbers that are the roots of nonzero polynomials with integer coefficients : countably infinite.

Since in the note polynomial with integers coefficient are countably infinite, we can enumerate them as $P_1, P_2, \ldots$. We can label each root for each polynomial as $(i, j)$ with $i$ denoting $P_i$, $j$ denoting $j^{th}$ root. After doing so, we know that all the roots are just subsets of $N \times N$ spaces, which is countably infinite.