CS 70 Discrete Mathematics and Probability Theory
Fall 2018 Alistair Sinclair and Yun Song

DIS 6A

1 Berlekamp-Welch Warm Up

(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 $1 \le i \le n$. 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.

2 Berlekamp-Welch Algorithm

In this question we will send the message $(m_0, m_1, m_2) = (4, 3, 2)$ of length $n = 3$. We will use an error-correcting code for $k = 1$ general error, doing arithmetic over GF(5).

(a) Construct a polynomial $P(x) \pmod 5$ of degree at most 2, so that

$$P(0) = 4, \qquad P(1) = 3, \qquad P(2) = 2.$$

What is the message $(c_0, c_1, c_2, c_3, c_4)$ that is sent?

(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 $Q(x)$ and $E(x)$.

(c) Assume that after solving the equations in part (b) we get $Q(x) = -x^2 + 4x$ and $E(x) = x$. Show how to recover the original message from Q and E.

Solution:

(a) We use Lagrange interpolation to construct the unique quadratic polynomial $P(x)$ such that $P(0) = m_0 = 4, P(1) = m_1 = 3, P(2) = m_2 = 2$.

$$\begin{aligned}
\Delta_0(x) &= \frac{(x-1)(x-2)}{(0-1)(0-2)} = \frac{x^2-3x+2}{2} \\
\Delta_1(x) &= \frac{(x-0)(x-2)}{(1-0)(1-2)} = \frac{x^2-2x}{-1} \\
\Delta_2(x) &= \frac{(x-0)(x-1)}{(2-0)(2-1)} = \frac{x^2-x}{2} \\
P(x) &= m_0\Delta_0(x) + m_1\Delta_1(x) + m_2\Delta_2(x) \\
&= 4\Delta_0(x) + 3\Delta_1(x) + 2\Delta_2(x) \\
&= -x + 4
\end{aligned}$$

[Note that all arithmetic is over GF(5), so for example $2^{-1} \equiv 3 \pmod 5$.] For the final message we need to add 2 redundant points of P. Since 3 and 4 are the only points in GF(5) that we have not used yet, we compute $P(3) = 1, P(4) = 0$, and so our message is $(4, 3, 2, 1, 0)$.

(b) The message received is $(c_0', c_1', c_2', c_3', c_4') = (0, 3, 2, 1, 0)$. Let $R(x)$ be the function such $R(i) = c_i'$ for $0 \le i < 5$. Let $E(x) = x + b_0$ be the error-locator polynomial, and $Q(x) = P(x)E(x) =$

$a_3x^3 + a_2x^2 + a_1x + a_0$. Since $Q(i) = P(i)E(i) = R(i)E(i)$ for $1 \le i < 5$, we have the following equalities $\pmod 5$:

$$\begin{aligned} Q(0) &= 0E(0) \\ Q(1) &= 3E(1) \\ Q(2) &= 2E(2) \\ Q(3) &= 1E(3) \\ Q(4) &= 0E(4) \end{aligned}$$

They lead to the following system of linear equations:

$$\begin{array}{rcrcrcrcrcl} & & & & & & a_0 & & & = & 0 \\ a_3 & + & a_2 & + & a_1 & + & a_0 & - & 3b_0 & = & 3 \\ 8a_3 & + & 4a_2 & + & 2a_1 & + & a_0 & - & 2b_0 & = & 4 \\ 27a_3 & + & 9a_2 & + & 3a_1 & + & a_0 & - & b_0 & = & 3 \\ 64a_3 & + & 16a_2 & + & 4a_1 & + & a_0 & & & = & 0 \end{array}$$

(c) From the solution, we know

$$\begin{aligned} Q(x) &= a_3x^3 + a_2x^2 + a_1x + a_0 = -x^2 + 4x, \\ E(x) &= x + b_0 = x. \end{aligned}$$

Since $Q(x) = P(x)E(x)$, the recipient can compute $P(x) = Q(x)/E(x) = -x+4$ [note that this is the same polynomial $P(x)$ from part (a) used by the sender]. The recipient may deduce the location of the error from $E(x)$ as follows. There is only one error at location e_1, we have $E(x) = (x - e_1) = x$, so $e_1 = 0$ and the error is at position 0. To correct the error we evaluate $P(0) = 4$. Since the other two positions m_1, m_2 of the message are uncorrupted, we recover the original message $(m_0, m_1, m_2) = (4, 3, 2)$.

3 Bijections

Consider the function

$$f(x) = \begin{cases} x, & \text{if } x \ge 1; \\ x^2, & \text{if } -1 \le x < 1; \\ 2x+3, & \text{if } x < -1. \end{cases}$$

(a) If the domain and range of f are $\mathbb{N}$, is f injective (one-to-one), surjective (onto), bijective?

(b) If the domain and range of f are $\mathbb{Z}$, is f injective (one-to-one), surjective (onto), bijective?

(c) If the domain and range of f are $\mathbb{R}$, is f injective (one-to-one), surjective (onto), bijective?

Solution:

(a) Yes, Yes, Yes: On $\mathbb{N}$, f is simply the identity function $id(x) = x$.

(b) No, No, No: Both -1 and 1 get mapped to 1 (hence not injective) and there is no $x \in \mathbb{Z}$ that gets mapped to -2 (hence not surjective).

(c) No, Yes, No: -1 and 1 still get mapped to 1 (hence not injective), but every value can be attained (since f is a continuous function and $\lim_{x\to\pm\infty} f(x) = \pm\infty$), so f is surjective.

4 Count It!

For each of the following collections, determine and briefly explain whether it is finite, countably infinite (like the natural numbers), or uncountably infinite (like the reals):

(a) $\mathbb{N}$, the set of all natural numbers.

(b) $\mathbb{Z}$, the set of all integers.

(c) $\mathbb{Q}$, the set of all rational numbers.

(d) $\mathbb{R}$, the set of all real numbers.

(e) The integers which divide 8.

(f) The integers which 8 divides.

(g) The functions from $\mathbb{N}$ to $\mathbb{N}$.

(h) Computer programs that halt.

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

Solution:

(a) Countable and infinite. See Lecture Note 10.

(b) Countable and infinite. See Lecture Note 10.

(c) Countable and infinite. See Lecture Note 10.

(d) Uncountable. This can be proved using a diagonalization argument, as shown in class. See Lecture Note 10.

(e) Finite. They are $\{-8,-4,-2,-1,1,2,4,8\}$.

(f) Countably infinite. We know that there exists a bijective function $f : \mathbb{N} \to \mathbb{Z}$. Then function $g(n) = 8f(n)$ is a bijective mapping from $\mathbb{N}$ to integers which 8 divides.

(g) Uncountably infinite. We use the Cantor's Diagonalization Proof:

Let $\mathscr{F}$ be the set of all functions from $\mathbb{N}$ to $\mathbb{N}$. We can represent a function $f \in \mathscr{F}$ as an infinite sequence $(f(0), f(1), \cdots)$, where the i-th element is $f(i)$. Suppose towards a contradiction that there is a bijection from $\mathbb{N}$ to $\mathscr{F}$:

$$\begin{aligned}
0 &\longleftrightarrow (f_0(0), f_0(1), f_0(2), f_0(3), \dots) \\
1 &\longleftrightarrow (f_1(0), f_1(1), f_1(2), f_1(3), \dots) \\
2 &\longleftrightarrow (f_2(0), f_2(1), f_2(2), f_2(3), \dots) \\
3 &\longleftrightarrow (f_3(0), f_3(1), f_3(2), f_3(3), \dots) \\
&\vdots
\end{aligned}$$

Consider the function $g : \mathbb{N} \to \mathbb{N}$ where $g(i) = f_i(i) + 1$ for $i \in \mathbb{N}$. We claim that the function g is not in our finite list of functions. Suppose for contradiction that it did, and that it was the n-th function $f_n(\cdot)$ in the list, i.e., $g(\cdot) = f_n(\cdot)$. However, $f_n(\cdot)$ and $g(\cdot)$ differ in the n-th number, i.e. $f_n(n) \neq g(n)$, because by our construction $g(n) = f_n(n) + 1$ (Contradiction!).

(h) Countably infinite. The total number of programs is countably infinite, since each can be viewed as a string of characters (so for example if we assume each character is one of the 256 possible values, then each program can be viewed as number in base 256, and we know these numbers are countably infinite). So the number of halting programs, which is a subset of all programs, can be either finite or countably infinite. But there are an infinite number of halting programs, for example for each number i the program that just prints i is different for each i. So the total number of halting programs is countably infinite. (Note also that this result together with the previous one in (g) implies that not every function from $\mathbb{N}$ to $\mathbb{N}$ can be written as a program.)

(i) Countably infinite. Polynomials with integer coefficients themselves are countably infinite. So let us list all polynomials with integer coefficients as $P_1, P_2, \dots$. We can label each root by a pair (i, j) corresponding to the j-th root of polynomial P_i (we can have an arbitrary ordering on the roots of each polynomial). This means that the roots of these polynomials can be mapped in an injective manner to $\mathbb{N} \times \mathbb{N}$ which we know is countably infinite. So this set is either finite or countably infinite. But every natural number n is in this set (it is the root of $x - n$). So this set is countably infinite.