Error Correcting Codes

Suppose that Alice wants to send to Bob a message over a noisy channel. One way would be to encode her message as a sequence $a_0a_1\cdots a_{N-1}$ of integers modulo a prime $p$ (think of $p$ as very big, much larger than the length $N$ of Alice’s message). The problem is, if she sends this sequence over the channel, her correspondent will receive an altered sequence $a_0'd_1'\cdots a'_N$, where up to $1/4$ of the integers have been changed.

There is a clever method based on the theory of polynomials over $\text{GF}_p$, the Berlekamp-Welsh code, for encoding her sequence in an error-correcting way, that is, such that the encoding will allow Bob to recover Alice’s original message even in the face of such high error rate.

First, given the original message $a_0a_1\cdots a_{N-1}$, Alice finds by Lagrange interpolation (the “sum-of-products” formula we saw in the previous lecture) the unique $N$-degree polynomial $f(x)$ such that $f(i) = a_i, i = 0, \ldots, N-1$. Then she sends over the noisy channel the message

$$a_0 = f(0), a_1 = f(1), a_2 = f(2), \ldots, a_{2N-2} = f(2N-2).$$

That is, she pads the $N$ given numbers with $N$ more values of the polynomial.

Of course, Bob at the other end receives a sequence $a_0'd_1'\cdots a'_N$, of numbers between 0 and $p-1$, with up to $\lfloor \frac{2N-1}{4} \rfloor = \frac{N}{2} - 1$ numbers changed. Unfortunately, Bob has no idea which digits were corrupted. (We assume that Bob received $2N - 1$ numbers in the same order as they were sent, and no number was omitted.) There is no way to interpolate a polynomial and recover $f$, because no polynomial of degree $N - 1$ goes through all these points.

Here are two important facts, however, that come to Bob’s rescue:

- If Bob were able to find an $N - 1$-degree polynomial that passes through $N + \frac{N}{2} - 1$ of the points, then this polynomial would be $f(x)$. Because, among the $N + \frac{N}{2} - 1$ points, at least $N + \frac{N}{2} - 1 - (\frac{N}{2} - 1) = N$ are correct, and there is only one polynomial that passes through these correct points — and we know that $f(x)$ does.

- Furthermore, there exists a polynomial like the one described above. Because out of the $2N - 1$ points, at least $2N - 1 - (\frac{N}{2} - 1) \geq N + \frac{N}{2} - 1$ points are correct, and we know that there is an $N - 1$-degree polynomial passing through these points — namely, $f(x)$.

So, from these two facts, we need to find, given $2N - 1$ points, an $N - 1$-degree polynomial that passes through $N + \frac{N}{2} - 1$ of the points (not all sets of $2N - 1$ points have such a polynomial, but we know that ours does).

Let us formulate our problem as a system of equations. We write $f(x)$ as $f_{N-1}x^{N-1} + \ldots + f_1x + f_0$, where the $f_j$’s are the unknown coefficients of the polynomial we are seeking. Then for each $x = 0, 1, 2, \ldots, 2N - 2$,

$$f_{N-1}x^{N-1} + \ldots + f_1x + f_0 = a'_x.$$
is an equation with unknowns the $f_i$'s. We have $2N - 1$ such equations, one for each $x = 0, 1, 2, \ldots, 2N - 2$, and we know that among them there is a set of $\frac{3N}{2} - 1$ equations that have a solution—but we still do not know which. We do not know where the errors occurred.

Although we know how to solve systems of linear equations, we do not know how to solve them when the variables are fewer than the equations, but some equations may be erroneous.

**Big idea:** Treat the points $e_1, \ldots, e_{\frac{N}{2} - 1}$ where the errors occurred as unknowns themselves, and rewrite the $2N - 1$ equations above as

$$(f_{N-1}x^{N-1} + \ldots + f_1x + f_0)(x - e_1)(x - e_2)\cdots(x - e_{\frac{N}{2} - 1}) = a'_e(x - e_1)(x - e_2)\cdots(x - e_{\frac{N}{2} - 1}).$$

Now these equations are all correct, for all $x = 0, 1, \ldots, 2N - 2$ because, when $x = e_i, i = 1, \ldots, \frac{N}{2} - 1$, and therefore $a'_e$ may not be equal to $a_e$, then the equation becomes $0 = 0$.

We are almost done: The polynomial in the left-hand side $(f_{N-1}x^{N-1} + \ldots + f_1x + f_0)(x - e_1)(x - e_2)\cdots(x - e_{\frac{N}{2} - 1})$ is a $N - 1 + \frac{N}{2} - 1$-degree polynomial $g(x)$, and thus it can be written as $g_{N+\frac{N}{2}-2}x^{N+\frac{N}{2}-2} + \ldots + g_1x + g_0$, and similarly the polynomial in the right-hand side is $(x - e_1)(x - e_2)\cdots(x - e_{\frac{N}{2} - 1}) = h_{\frac{N}{2}-1}x^{\frac{N}{2}-1} + \ldots + h_1x + h_0$. Thus, we have a system of $2N - 1$ equations with $2N - 1$ unknowns, and we can solve for the coefficients of $g(x)$ and $h(x)$, upon which we get the original message as the values of $g(x)/h(x)$ at the points $x = 0, 1, \ldots, N - 1$. (Division of polynomials is not much harder than long division.)