Note I.23: Alice, Bob, and Coding Bounds

2/5

First, let's construct the OGF for all allowed codewords, which are sequences (encoded strings) not containing 11. Then, use the rational function transfer theorem to find the number of such sequences of length L:

What if you just have "1"? Or "101"?

$$C(z) = SEQ(Z_0 + Z_1 Z_0)$$

The OGF is (1+z)/(1-z-z^2)

$$C(z) = \frac{1}{1-z-z^2} = \frac{f(z)}{g(z)} \text{ where } f(z) = 1,\ g(z) = 1 - z - z^2$$

The denominator $g(z)$ has root $\frac{1-\sqrt{5}}{2}$ so $\beta = \frac{1+\sqrt{5}}{2}$:

-1

$$[z^L]C(z) \sim \frac{-\beta f(1/\beta)}{g'(1/\beta)}\beta^L = \frac{-\beta(1)}{-1-\frac{2}{\beta}}\beta^L$$

$$= \frac{\beta^{L+1}}{1+2(\frac{1}{\beta})}$$

$$= \frac{1}{2-\sqrt{5}}(\beta)^{L+1}$$

$$= (2+\sqrt{5})(\beta)^{L+1}$$

Since we must have a one-to-one mapping of plaintext strings length n to codewords of length L, use the given equality and solve for L in terms of n:

You want to bound the sum of C_j since there are codewords of all lengths less than or equal to L

$$2^n \le (2+\sqrt{5})(\beta)^{L+1}$$

$$n \le (L+1)lg(\beta) - lg(2-\sqrt{5})$$

-2

$$L + 1 \ge \frac{n}{lg(\beta)} + lg(some\ constant)$$

$$L \ge \frac{n}{lg(\beta)} + O(1)$$

Thus $L \ge \lambda n + O(1)$ as shown