15-251: Great Theoretical Ideas In Computer Science

Recitation 14

Definitions and Review

- **Polynomials & Lagrange Interpolation.** We can represent a degree-d polynomial $P(X) \in F[X]$ in 2 different ways:

  (a) As P's $d+1$ coefficients, or

  (b) As P's values on $d+1$ different field elements.

  We can convert between (a) $\rightarrow$ (b) by evaluating P on $d+1$ elements, and between (b) $\rightarrow$ (a) using Lagrange interpolation.

- **Reed-Solomon Encoding.** If Alice has a message of $d+1$ elements of field F, she can think of it as the coefficients of a degree-d polynomial $P(X)$, and encode $P(X)$ using its values representation. To guard against at most k erasures, she can send $d+k+1$ symbols; if there are up to k corruptions, she can send $d+2k+1$ symbols.

- **Hamming(7,4).** Suppose Alice wants to send a 4-bit message while guarding against 1 bitflip. By using Hamming (7,4) code she can send Bob 7 bits. If there is an error, Bob will be able to detect where the error is and recover Alice's message.

- **Generating Function.** The generating function for a sequence $V = \langle a_0, a_1, a_2, ..., a_n, ... \rangle$ is the formal power series $P(X) = \sum_{i=0}^{\infty} a_i X^i$.

- **Convolution Rule.** Suppose we have disjoint sets A and B. Let $A(X)$ be the generating function for selecting items from A, and let $B(X)$ be the same thing for B. The number of ways to select n items from $A \cup B$ is $(a_0 b_n + a_1 b_{n-1} + a_2 b_{n-2} + ... + a_n b_0)$. The generating function for selecting items from $A \cup B$ is simply $A(X)B(X)$.

more hamming

Here's a simple example of how to generalize Hamming code. Suppose Alice wants to send a longer message to Bob using Hamming code. Let's say that Bob has received 15 bits from Alice. How many bits long is Alice's original message? What does Bob's "check matrix" H look like? Finally, how many possible messages could Alice have sent using her 15 bits?

reed-solomon practice

A nice and smart cat wants to send us a message consisting of 3 numbers $m_0, m_1, m_2 \in F_{11}$. The channel he will send over is very noisy, so he uses Reed-Solomon encoding. He interprets his message as the coefficients of a polynomial $P(x) = m_0 + m_1 x + m_2 x^2$, evaluates this polynomial on all eleven elements in F_{11}, and sends the results $P(0), \ldots, P(10)$.

Suppose that, because of noise, we cannot make out some of the numbers sent; i.e., we receive

$$(??, y_1 = P(1), ??, ??, ??, y_5 = P(5), ??, y_7 = P(7), ??, ??, ??, ??).$$

(a) Luckily this is enough for us to decode the message. Decode the message for $y_1 = 0$, $y_5 = 8$, $y_7 = 6$.

(b) Consider if the cat did his eleven polynomial evaluations mod 12 rather than mod 11. Suppose we received the same information from the cat as above. Can we still recover his message? Why or why not?

generating functions

(a) Find the generating function for the sequence $1, 1, 1, 1, \ldots$. in closed form.

(b) What's the coefficient of x^{2005} in the generating function $G(x) = \frac{1}{(1+x)^2(1-x)^2}$?

(c) We have 20 bags, each bag containing a 5 dollar coin and a 7 dollar coin. If we can use at most one coin from each bag, in how many ways can we make 17 dollars, assuming that all coins are distinguishable (i.e. the 5 dollar coin from the first bag is considered to be different from that in the second bag, and so on)?

(d) Using generating functions, find a_n in terms of n:
$a_0 = 2$ and $a_{n+1} = 3a_n$ for $n \geq 0$.

2-50-*∼fun∼*

251 is fun! In fact, it's so fun, everyone is jealous of all the 251 students. There is going to be a secret party, and invitations with the secret entrance password are being sent over the internet. The password is three one-digit numbers less than 7 and is encoded as a polynomial f of degree 2 in F_7. However, the internet channel at CMU is so noisy that the mastermind of the party decided to use RS Code to send out the message. You are one of the jealous ones and intercept a message of $(1, 1, 5, 6, 1) = (y_0, \ldots, y_4)$, and you know that at most one of the numbers in the message has been altered by the noisy channel. You also know that the mastermind originally sent the message $(f(0), f(1), f(2), f(3), f(4))$. Figure out what the password is so that you can secretly attend the secret party of 2-50-fun.