Error Correcting Codes: Combinatorics, Algorithms and Applications (Spring 2009)

Lecture 12: Reed Solomon Codes and Communication Complexity

February 9th, 2009

Lecturer: Atri Rudra *Scribe: Krishna Ramkumar*

In the last lecture, we talked about explicit codes and introduced Reed Solomon codes. We also proved that Reed Solomon codes meet the Singleton bound and hence are Maximum Distance Separable (MDS).

In today's lecture, we shall prove another interesting property of an MDS code $C \subseteq \Sigma^n$ with integral dimension k.

1 A Property of MDS Codes

Definition 1.1. *For any subset of indices $S \subseteq [n]$ of size exactly k and $C \subseteq \Sigma^n$, C_S is all the codewords in C projected onto the indices in S.*

Proposition 1.2. *Let $C \subseteq \Sigma^n$ of dimension k be an MDS code, then for all $S \subseteq [n]$ such that $|S| = k$, we have $|C_S| = \Sigma^k$.*

Let us now proceed to see a proof for Reed Solomon Codes which is presented below.

Proof for Reed Solomon Codes. Consider any $S \subseteq [n]$ of size k and fix an arbitrary $v \in \mathbb{F}_q^k$, there exists a codeword $c \in RS$ such that $c_S = v$. Consider a generic degree $k-1$ polynomial $P(X) = \sum_{i=0}^{k-1} p_i X^i$.

We need to show that there exists $P(X)$ such that $P(\alpha_i) = v_i$ forall $i \in S$, where $|S| = k$. For this, think of p_i's as unknowns in the equations that arise out of the relations $P(\alpha_i) = v_i$. In other words, consider:

$$\begin{pmatrix} p_0 & p_1 & \ldots\ldots p_{k-1} \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_i & \alpha_k \\ \alpha_1^2 & \alpha_i^2 & \alpha_k^2 \\ . & . & . \\ . & . & . \\ . & . & . \\ \alpha_1^{k-1} & \alpha_i^{k-1} & \alpha_k^{k-1} \end{pmatrix} = \begin{pmatrix} v_1 \\ . \\ . \\ . \\ . \\ . \\ v_k \end{pmatrix}$$

The above matrix is a Vandermonde matrix and thus, has full rank. Hence, there always exists a solution for $(p_0, \ldots\ldots\ldots, p_{k-1})$. This completes the proof for Reed-Solomon codes, the proof for the general case is dealt with below.

□

Proof of Proposition 1.2. Consider a $|C| \times n$ matrix where each row represents a codeword in C. Hence, there are $|C| = \Sigma^k$ rows in the matrix. The number of columns is equal to the block length n of the code. Since C is Maximum Distance Separable, its distance $d = n - k + 1$.

Let $S \subseteq [n]$ be of size exactly k. It is easy to see that for any $c^i \neq c^j \in C$, the corresponding $c^i_S \neq c^j_S \in C_S$. As otherwise $\triangle(c^i, c^j) \leq d-1$, which is not the case because we have the minimum distance of the code C to be d. Therefore, every codeword in C gets mapped to a distinct codeword in C_S. As a result $|C_S| = |C| = \Sigma^k$. As $C_S \subseteq \Sigma^k$, this implies that $C_S = \Sigma^k$ as desired. □

2 Communication Complexity

Communication complexity is a mathematical theory developed to study the communication processes in several aspects of computation. Today we will look at the simple two-party model introduced by Yao in 1979, which is still the most widely studied model. The treatment here follows the one in [1]. Yao's model makes the following simplifying assumptions:

- There are only two parts in the system.
- Each part of the system gets a fixed part of the input information.
- The only resource we care about is communication
- The task is the computation of some prespecified function of the input.

In the two party communication model that we look at today, there are two parties, Alice and Bob at each end of the communication channel. Alice knows $x \in \{0,1\}^n$ and Bob knows $y \in \{0,1\}^n$. Alice and Bob exchange bits over the communication channel between them according to a fixed protocol P until the value of $f(x, y)$ (Here, $f(x, y)$ is some arbitrary function in x and y)is known. The problem is formalized below.

Goal: Given $f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$. At the end of the communication process, Alice and Bob should know $f(x, y)$. Communicate as few bits as possible in order to compute $f(x, y)$.

Also, at each stage of the communication process, the protocol P must determine whether the run terminates; if the run has terminated, the protocol must specify the answer given by the protocol i.e. $f(x, y)$; and if the run has not terminated, the protocol must specify who sends the next bit. The protocol should do this based on the bits communicated so far, as there is no other knowledge common to both Alice and Bob. The protocol, at every stage of the communication, must also specify what each player needs to send (this depends on the communication so far and the players' input).

Our focus is on the amount of communication between the two parties and so we ignore the internal computation each of them makes. The cost of a protocol P on input (x, y) is the number of bits communicated.

Definition 2.1. *The cost of a protocol P is the worst case cost over all inputs (x, y).*

Any f can be decided in $\leq n + 1$ bits. This is easy to see as either Alice or Bob can send their entire input to the other using n bits and since we assume that there is no limitation on internal computation resources at each end, the function f can be computed and the result bit can be exchanged using one bit. The question is, can we do better? We formalize this question by defining the communication complexity of a function.

Definition 2.2. *$CC(f)$ is the minimum number of bits exchanged over all protocols that decide f.*

Given a function f, the motivation is to design better protocols and hence reduce the communication complexity.

Towards the end of the lecture, the following functions (in all the cases below $x, y \in \{0, 1\}^n$) were mentioned whose communication complexity, we will discuss in the next lecture.

1. $f_1(x, y) = 1$ if and only if $\Sigma_i x_i \neq \Sigma_i y_i$ (the sums are over $\mathbf{F}_2$)
2. $f_2(x, y) = 1$ if and only if $\mid x \mid + \mid y \mid \geq t$ (where $\mid x \mid$ denotes the Hamming weight of x and $t \geq 1$ is an integer)
3. $f_3(x, y) = 1$ if and only if $x \geq y$ (where we think of x and y as integers)
4. $f_4(x, y) = 1$ if and only if $x_i = y_i$ for every $i \in [n]$
5. $f_5(x, y) = 1$ if and only if $x_i y_i = 0$ for every $i \in [n]$

The functions f_4 and f_5 are known as (set) equality and (set) disjointness in the literature. The connections to sets comes from the observation that any vector in $\{0, 1\}^n$ can be thought of as the characteristic vector of a subset of $\{1, ..., n\}^n$.

3 References

1. Eyal Hushilevitz and Noam Nisan: *Communication Complexity*, Cambridge University Press 1997.