CS 6815 Pseudorandomness and Combinatorial Constructions **Fall 2019**

Lecture 13: October 10

Lecturer: Jesse Goodman *Scribe: Abhishek Shetty*

13.1 Motivation and Definitions

Consider the following scenarios:

- Two players are communicating on a noisy channel in which a few of the bits of the message can be altered. Can they still get reliable communication?
- Data is stored on a disk and a few locations in the memory can be altered. Can the disk be read reliably?

A natural idea to deal with these scenarios would be to add redundancy to make sure that the message can be recovered even when the symbols at a few locations are altered. An abstraction that captures this intuition is that of error correcting codes. Before defining them, we first look at some preliminary definitions.

Definition 13.1 (Hamming distance)**.** *Let Σ be a finite alphabet. For two strings x and y of length n, we define the Hamming distance between them as*

$$\Delta(x, y) = \left|\{i : x_i \neq y_i\}\right|.$$

We denote by $B(x, \alpha) = \{y : \Delta(x, y) \leq \alpha\}$ the Hamming ball of radius α around x.

Intuitively, an error correcting code can be thought of as a mechanism that maps strings of a small length to strings of longer length such that even when some of the locations in the coded message are tampered with, we can recover the original message. We would also like efficient encoding and decoding algorithms for the code, but in this lecture we will focus just on the set of codewords. This leads to the following definition.

Definition 13.2 (Error Correcting Codes)**.** *Let Σ be a finite alphabet. An error correcting code C is a subset of Σ^n. The elements of C are known as the codewords. Associated with any such code are the following parameters:*

- *Alphabet size $q = |\Sigma|$*
- *Block length n*
- *Dimension $k = \log_q |C|$*
- *Minimum distance $d = \min_{x \neq y; x, y \in C} \Delta(x, y)$*
- *Rate $r = k/n$*
- *Relative distance $\delta = d/n$*

A code with block length n, dimension k and minimum distance d on an alphabet of size q is referred to as a $(n, k, d)_q$ code.

Next, we note the error correction and error detection properties of ECCs. First, note that if an error is such that it does not change a codeword to another, we can detect that an error has occured. Thus, we can detect upto $d-1$ errors, since the minimum number of changes that need to be made to convert one codeword to another is d. Next, note that for any $x, y \in C$, $B\left(x, \left\lfloor \frac{d-1}{2} \right\rfloor\right) \cap B\left(y, \left\lfloor \frac{d-1}{2} \right\rfloor\right)$ is empty. Thus, we can correct upto $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors by outputing the closest codeword to the given string (though, it is not clear that this can be done efficiently).

13.2 Tradeoff between Parameters

From the definitions, it is clear that we would like to construct codes with high rate and high relative distance. In the following theorem, we note a tradeoff between these parameters.

Theorem 13.3 (Singleton Bound)**.** *Let C be a code with alphabet size q, block length n, dimension k and distance d. Then,*

$$k \leq n - d + 1.$$

Proof. We will show that $|C| \leq q^{n-d+1}$. Towards a contradiction, assume that $|C| > q^{n-d+1}$. Since, there are only q^{n-d+1} different words of length $n-d+1$, there are two distinct codewords x, y that agree on their initial $n-d+1$ block. Then,

$$\Delta(x, y) \leq n - (n - d + 1) \leq d - 1.$$

This contradicts the minimum distance of the code. □

Restating this in terms of the rate and relative distance, we get

$$r \leq 1 - \delta + \frac{1}{n}.$$

13.3 Linear Codes

Definition 13.4 (Linear Codes)**.** *A code C is said to be linear if the alphabet is a finite field $\mathbb{F}_q$ and C is a subspace of $\mathbb{F}_q^n$. In this case, the dimension of the code corresponds to the dimension of C as a subspace of $\mathbb{F}_q^n$. A linear code with block length n, dimension k and minimum distance d on an alphabet of size q is referred to as a $[n, k, d]_q$ code.*

Definition 13.5. *Let $C \subseteq \mathbb{F}_q^n$ be a linear code of dimension k. A matrix $G \in \mathbb{F}_q^{n \times k}$ is said to be generator matrix if its columns span C. A matrix H is said to be a parity check matrix if $H(C) = 0$ i.e. C is the kernel of H.*

Definition 13.6. *Let $C \subseteq \mathbb{F}_q^n$ be a linear code of dimension k. Then, the dual code $C^\perp$ is a code with dimension $n-k$ defined as*

$$C^\perp = \left\{x : \forall y \in C, \langle x, y \rangle = 0\right\},$$

where $\langle \cdot, \cdot \rangle$ is the usual inner product given by $\langle x, y \rangle = \sum_{i=1}^n x_i y_i$.

Note that since finite fields have finite characteristic, there are elements $x \in \mathbb{F}_q^n$, such that $\langle x, x \rangle = 0$. In particular, the intersection of C and $C^\perp$ can be non-empty.

Let $G^\perp$ be the generator matrix of the dual code. Then, for all $x \in C$, $\left(G^\perp\right)^T x = 0$ since the rows of $G^\perp$ are orthogonal to x. Thus, $\left(G^\perp\right)^T$ is a parity check matrix for C. Also, note that $\left(C^\perp\right)^\perp = C$. From this and the previous fact it follows that G^T is a parity check matrix for $C^\perp$.

Next, we express the minimum distance of linear codes in an alternate way.

Lemma 13.7. *Let C be any linear code with minimum distance d, then*

$$d = \min_{C \ni x \neq 0} \|x\|_0 = \min_{C \ni x \neq 0} \left|\{i : x_i \neq 0\}\right|.$$

Proof. Let x, y be the codewords that attain the minimum distance of the code. Then, note that since C is a linear code, $x - y \in C$ and $\|x - y\|_0 = \Delta(x, y)$. Similarly, let z be a vector with the minimum non-zero entries. Since C is a linear code $0 \in C$. Thus, $\Delta(z, 0) = \|z\|_0$ as required. □

13.4 Examples of Codes

13.4.1 Hadamard Code

Definition 13.8 (Hadamard Code)**.** *Let $m \in \mathbb{Z}^+$. Then, the Hadamard code is the set of linear functions from $\mathbb{F}_2^m$ to $\mathbb{F}_2$ seen as vectors in $\mathbb{F}_2^{2^m}$. That is,*

$$H(m) = \left\{ \left(\langle x, y \rangle\right)_{y \in \mathbb{F}_2^m} : x \in \mathbb{F}_2^m \right\}.$$

In words, a vector in the Hadamard code corresponds to the truth table of a linear function with each coordinate corresponding to the evaluation of the function at a point in $\mathbb{F}_2^m$. The fact that the Hadamard code is linear is clear from the definition. The generator matrix of the Hadamard code is given by

$$G = \begin{bmatrix} y_{1,1} & y_{1,2} & y_{1,3} & \cdots & y_{1,m} \\ y_{2,1} & y_{2,2} & y_{2,3} & \cdots & y_{2,m} \\ y_{3,1} & y_{3,2} & y_{3,3} & \cdots & y_{3,m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ y_{2^m,1} & y_{2^m,2} & y_{2^m,3} & \cdots & y_{2^m,m} \end{bmatrix},$$

where y_i represents the i-th element in $\mathbb{F}_2^m$ and $y_{i,j}$ represents the j-th location of the i-th string.

Lemma 13.9 (Parameters of the Hadamard Code)**.** *The Hadamard code $H(m)$ is a $\left[2^m, m, 2^{m-1}\right]_2$ code.*

Proof. The dimension and block length follow from the definition. Next we show that for any non-zero linear function $f(x) = \sum_{i=1}^m x_i y_i$ has exactly 2^{m-1} zeros. This can be seen by noting that since the rank of f is 1, the kernel of f has dimension $m - 1$ and that a $m - 1$-dimensional subspace over $\mathbb{F}_2$ has size 2^{m-1}. □

From this, we see that though the Hadamard code has exceptional relative distance of $1/2$, it has a poor rate of $m2^{-m}$.

13.4.2 Reed–Solomon Code

Definition 13.10 (Reed-Solomon Code)**.** *Let $Q \subset \mathbb{F}_q$ and let $r < |Q| = m$. Then, Reed–Solomon code $RS_q(r)$ is given by evaluations of $\mathbb{F}_q$ polynomials of degree at most r on Q. That is*

$$RS_q(r) = \left\{ \left(f(y)\right)_{y \in Q} : f \in \mathbb{F}_q[x] \ \textit{ with } deg(f) \leq r \right\}.$$

Since the sums and scalar multiples of polynomials of degree at most r is also a polynomial of degree r, we have that the Reed–Solomon codes are linear. The generator matrix of the Reed–Solomon code is given by

the Vandermonde matrix defined by Q. That is,

$$G = \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^r \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^r \\ 1 & \alpha_3 & \alpha_3^2 & \dots & \alpha_3^r \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_m & \alpha_m^2 & \dots & \alpha_m^r \end{bmatrix},$$

where $Q = \{\alpha_1 \dots \alpha_m\}$.

Lemma 13.11 (Parameters of the Reed–Solomon Code)**.** *The Reed–Solomon code $RS_q(r)$ is a $[m, r+1, m-r]_q$ code.*

Proof. Since a non-zero polynomial of degree at most r, can have at most r zeroes, two distinct polynomials cannot agree on all points of Q. Thus, the dimension of the Reed–Solomon code is $r+1$. Furthermore, each such non-zero vector can have at most r zeroes. Thus, the minimum distance is $m-r$. □

Note that the Reed–Solomon code meets the singleton bound and in that sense they are optimal. But, one disadvantage is that the block length of the code can be at most the alphabet size which we would usually like to keep small. In the next lecture, we will see the Reed–Muller codes which naturally generalize both these codes.