Lecture 3: Hadamard codes, BCH codes, Reed-Solomon codes

Topics in Error-Correcting Codes (Fall 2022)
University of Toronto
Swastik Kopparty
Scribe: Craig Belair and Kunal Chawla

1 The Hadamard Code

In the previous lecture we introduced the **Plotkin Bound**. We determined that, for $C \subseteq \{0,1\}^n$:

Proposition 1. *If C has distance $d \geq \frac{n}{2}$, then $|C| \leq O(n)$.*

Proposition 2. *If C has distance δn, then the rate, R of the code C satisfies $R + 2\delta \leq 1 + o(1)$.*

We proved the first by embedding our code into $\mathbb{R}^n$ and using the following fact:

Fact 3. *If $v_1, ..., v_k \in \mathbb{R}^n$ is a collection of vectors with $\langle v_i, v_j \rangle \leq 0$ for any $i \neq j$, then $k \leq 2n$.*

This bound is sharp: the collection of vectors $\pm e_1, ..., \pm e_n$ attains the $2n$ bound. Is the corresponding bound on codes also sharp? For now, we will show that if $n = 2^t - 1$, $\Sigma = \{0,1\}^n$, then there exists a linear code C of distance $d = \frac{n+1}{2}$ with $|C| = n + 1$. The type of code we will present is known as a **Hadamard Code**.

Let M be a $t \times 2^t - 1$ matrix whose columns are comprised of the nonzero elements of $\mathbb{F}_2^t$:

$$M = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,2^t-1} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,2^t-1} \\ \cdots & \cdots & \cdots & \cdots \\ a_{t,1} & a_{t,2} & \cdots & a_{t,2^t-1} \end{bmatrix}$$

Let C be the code generated by the matrix M. That is, for any $x \in C$, $x = aM$ where $a \in \mathbb{F}_2^t$. Recall that the **Hamming Code** was defined as $\{x : Mx^T = \overrightarrow{0}\}$ for a matrix M as in our example. It follows that if $k \in H$ (where H is the **Hamming Code** of the matrix M) and $x \in C$, then $k \cdot x = 0$. That is, the **Hadamard Code**, C, is the space orthogonal to the **Hamming Code**.

Claim: C as described above has size 2^t.

Proof. Suppose $f_1, f_2 \in \mathbb{F}_2^t$ with $f_1 \neq f_2$, but $f_1 M = f_2 M$. Then $(f_2 - f_1)M = \overrightarrow{0}$. But if $f_2 \neq f_1$ then $f_2 - f_1$ has at least one nonzero coordinate. Suppose the i'th coordinate of $f_2 - f_1$ is nonzero. By construction, M has a column with all zero entries except the $i'th$ coordinate, call that the $j'th$ column. Then the $j'th$ coordinate of $(f_1 - f_2)M$ is nonzero, contradicting our above conclusion. Thus for any $f_1, f_2 \in \mathbb{F}_2^t$ with $f_1 \neq f_2$, we have $f_1 M \neq f_2 M$. It follows that $|C| = |\mathbb{F}_2^t| = 2^t$. □

Claim: For any $y \in \mathbb{F}_2^t$ with $y \neq \overrightarrow{0}$, it is the case that a yM has **Hamming Weight** of $k \geq 2^{t-1} > \frac{n}{2}$. Hence the distance of the code C described above is at least $\frac{n}{2}$.

Proof. The columns of M are indexed by the elements of $\mathbb{F}_2^t/\{0\}$. So for any $y \in (\mathbb{F}_2^t/\{0\})$, the $i'th$ coordinate of yM is $\langle x, y\rangle$ where x is the element of $\mathbb{F}_2^t$ that makes up the $i'th$ column of M. The question of how many coordinates of yM are zero is then equivalent to asking how many distinct elements of S exist where:

$$S = \{x \in (\mathbb{F}_2^t/\{0\}) : \langle x, y\rangle = 0\}$$

Since $y \neq 0$, the linear map $\mathbb{F}_2^t \to \mathbb{F}_2$ given by $x \to \langle x, y\rangle$ is surjective. Hence by rank-nullity the set S has size $2^{t-1} - 1$. It follows that the **Hamming Weight** of yM is equal to the number of coordinates of yM, subtract away the number of coordinates which are 0:

$$Ham(yM) = (2^t - 1) - |S| = 2^t - 1 - (2^{t-1} - 1) = 2^{t-1} = \frac{n+1}{2} > \frac{n}{2}$$

Since C is a linear code, we can conclude that it was distance at least $n/2$. □

Definition 4. *An* ***Affine Hadamard Code*** *is a code of length* $n = 2^t$*, with coordinates identified with* $\mathbb{F}_2^t$ *:*

$$C = \{f : \mathbb{F}_2^t \to \mathbb{F}_2, f(x) = \langle x, y\rangle + b \text{ for some } y \in \mathbb{F}_2^t, b \in \mathbb{F}_2\}$$

These attain the sharp bound $|C| = 2^{t+1} = 2n$

Exercise 5. *How would the construction of* ***Hadamard Codes*** *work if we use* $\mathbb{F}_p$ *for a general p, instead of* $\mathbb{F}_2$*? How do the resulting expressions for* $|C|$ *and distance d differ from the expressions we found using* $\mathbb{F}_2$*?*

2 More on the Plotkin Bound

We aim to prove proposition 2, the second part of the Plotkin bound. The proof is applying the first part of the Plotkin bound to a collection of subcodewords of length $2\delta n$.

Proof. Suppose a code C over $\Sigma = \{0, 1\}$ has distance δn. For each $c \in C$, represent $c = (c_1, c_2) \in \Sigma^{(1-2\delta)n)} \times \Sigma^{2\delta n}$. Define:

$$B_{c_i} := \{c = (c_i, c_2) : c \in C\}$$

Then find some j such that $|B_{c_j}| \geq |B_{c_i}|$ for all $c_i \in \Sigma^{(1-2\delta)n}$. That is, c_j is the most popular (or tied with the most popular) choice for the first $(1 - 2\delta)n$ bits of elements of C. There are $2^{(1-2\delta)n}$ (not necessarily nonempty) such sets B, and they partition C, so that

$$|B_{c_j}| \geq \frac{|C|}{2^{(1-2\delta)n}}.$$

Further, we know that the $c_2's$ in B_{c_j} form a distance δn code of length $2\delta n$, hence by proposition 1, $|B_{c_j}| \leq 4\delta n$.

Rearranging, we get $|C| \leq 4\delta n 2^{(1-2\delta)n}$. Taking logs, we get

$$R := \frac{\log_2 |C|}{n} \leq 1 - 2\delta + o(1).$$

□

3 The Singleton Bound

Proposition 6. *Over any finite alphabet Σ, any code C of rate R and relative distance δ satisfies*

$$R + \delta \leq 1 + o(1).$$

Proof. As in the proof of proposition 2, for each $c \in C$, represent c as (c_1, c_2) where $c_1 \in \Sigma^{(1-\delta)n}$ and $c_2 \in \Sigma^{\delta n}$. Again, define:

$$B_{c_i} := \{c = (c_i, c_2) : c \in C\}.$$

Find some c_j such that $|B_{c_j}| \geq |B_{c_i}|$ for all $c_i \in \Sigma^{(1-\delta)n}$. Then B_{c_j} contains a code of length δn and distance δn. It follows that all elements of B_{c_j} must have c_2 components which share no common coordinates. So the maximum number of possible elements of B_{c_j} is the number of distinct characters in the alphabet, that is, $|\Sigma|$. Thus:

$$|C| \leq |\Sigma|^{(1-\delta)n+1}.$$

Note that $R = \frac{\log_{|\Sigma|}(|C|)}{n} \implies |\Sigma|^{Rn} = |C|$. Substituting this into the previous inequality yields $|\Sigma|^{Rn} \leq |\Sigma|^{(1-\delta)n+1} \implies Rn \leq (1-\delta)n + 1 \implies R + \delta \leq 1 + \frac{1}{n} = 1 + o(1)$ □

4 Reed-Solomon Codes:

Every time we see an inequality in the wild, we should ask whether it is sharp. In the singleton bound sharp in any reasonable sense? It turns out it is, but to see why we need to change out point-of-view a bit. Whenever we analyze codes in this course, we're always letting some parameter go to infinity, and working over a fixed alphabet. In this example, we'll let the size of our alphabet go to infinity.

Consider the **Reed-Solomon Code**. Let $\Sigma = \mathbb{F}_p$ for some prime p. Let the string length, $n = p$, and let $k = (1-\delta)p$. Then define a code C as the space of polynomial functions of degree $\leq k - 1$. In other words:

$$\mathrm{RS}_k := \{f : \mathbb{F}_p \to \mathbb{F}_p, f(x) = \sum_{i=0}^{k} a_i x^i\}.$$

Here, we're identifying our coordinates with elements of $\mathbb{F}_p$.

Observation 7. *The Reed-Solomon code* RS_k *is a linear code of size* p^{k+1}.

Proposition 8. *The Reed-Solomon code* RS_k *has distance* δp.

Proof. Since RS_k is a linear code, it suffices to show that every nonzero element has Hamming weight $\geq \delta p$. If not, there exists a polynomial of degree $k < p$ with strictly more than $(1-\delta)p = k$ roots, a contradiction. □

The contradiction comes from the following fact:

Fact 9. *Any nonzero polynomial* P *of degree* d *over a field* $\mathbb{F}$ *has at most* d *roots.*

Proof. Let a be a root, then $P = (x-a)Q(x)$ for some Q of degree $d-1$. We're done by induction. □

The Reed-Solomon code has rate $1 - \delta - \frac{1}{p}$, and distance δ. Hence as $p \to \infty$, the singleton bound is saturated.

5 Dual of Reed-Solomon Codes

The dual of the Hamming code had nice properties. Let's look at the dual of the Reed-Solomon code RS_k:

$$\mathrm{RS}_k^{\perp} = \{g : \mathbb{F}_q \to \mathbb{F}_q : \langle g, f\rangle = 0 \text{ for all } f \in \mathrm{RS}_k\}.$$

By finite-field shenanigans, this is also a Reed-Solomon Code!

Theorem 10. $RS_k^{\perp} = \mathrm{RS}_{q-k-2}$.

Proof. Observe that $\dim \mathrm{RS}_k = k+1$, that $\dim \mathrm{RS}_{q-k-2} = q-k-1$, and the space of functions $\mathbb{F}_q \to \mathbb{F}_q$ has dimension q, so it suffices to show the two spaces are orthogonal.

Notice that for any j, the space RS_k is spanned by $\{x^i\}_{i=0}^{i=k}$, so really it suffices to show that for any $a \leq q-2$, we have

$$\sum_{x \in \mathbb{F}_q} x^a = 0.$$

We can really take the sum over $x \neq 0$. Recall that the multiplicative group of any finite field is cyclic, so pick a generator $g \in (\mathbb{F}_q)^{\times}$. Then we can rewrite the sum as

$$\sum_{\ell=1}^{q-1}(g^\ell)^i = \frac{g^i - g^{iq}}{1-g} = 0.$$

□

This last step seems a little magical to me, so here's an alternate proof that $\sum_{x\in\mathbb{F}_q} x^i = 0$ for any $i \leq q-2$. At it's core it's really a rephrasing of the previous proof, but it avoids mentioning the fact that $(\mathbb{F}_q)^\times$ is cyclic.

Proof. For $i \in \{0, ..., q-2\}$, denote $S_i = \sum_{x\in\mathbb{F}_q} x^i$. For nonzero $a \in \mathbb{F}_q$, the map $x \to ax$ is bijective, so that $S_i = a^i S_i$. If S_i is nonzero, this implies that $a^i = 1$ for all nonzero a. This is a contradiction since the polynomial $x^i - 1 = 0$ has at most $i \leq q-2$ roots. □

6 A Parity Check Matrix for full Reed-Solomon Codes

As an immediate consequence of Theorem **??**, we can construct a parity-check matrix G_k for Reed-Solomon Codes:

$$q-k-1 \text{ rows}\left\{\overbrace{\begin{pmatrix} & & 1 & \\ & & \alpha & \\ \cdots & \cdots & \alpha^2 & \cdots \\ & & \vdots & \\ & & \alpha^{q-k-2} & \end{pmatrix}}^{q \text{ columns}}\right.$$

Here the columns are indexed by elements of $\mathbb{F}_q$. Each row is a basis vector for RS_k. By theorem **??**, the subspace RS_k is precisely the kernel of this matrix. We'll use the following lemma:

Lemma 11. *For any distinct $\alpha_1, ..., \alpha_k$, the Vandermonde matrix*

$$\begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_k \\ \alpha_1^2 & \alpha_2^2 & \alpha_2^2 & \dots & \alpha_3^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-i1} & \alpha_2^{k-1} & \alpha_3^{k-1} & \dots & \alpha_k^{k-1} \end{bmatrix}$$

has nonzero determinant.

Proof. Observe that the determinant of this matrix is a polynomial in $\alpha_1, ..., \alpha_k$. Writing the determinant as a sum over permutations, each term has degree $1 + 2 + ... + (k-1) = \binom{k}{2}$. Since the determinant is alternating, then it is 0 whenever $\alpha_i = \alpha_j$. In particular, the determinant is divisible by $\prod_{i<j}(\alpha_j - \alpha_i)$. Since this latter polynomial has degree $\binom{k}{2}$, we are done. □

Observation 12. *The Reed-Solomon code* RS_k *has distance* k.

Proof. Since RS_k is a linear code, it suffices to check that the Hamming weight of every nonzero codeword $f \in \mathrm{RS}_k$ is at least k. Suppose not, then there exists a nonzero codeword x supported on fewer than k coordinates such that $G_k \cdot x = 0$. Let $\alpha_1, ..., \alpha_k \in \mathbb{F}_q$ correspond to these k coordinates (if x is supported on fewer coordinates, choose any distinct α's to complete the list).

Then the Vandermonde matrix on $\alpha_1, ..., \alpha_k$ has nontrivial nullspace. In particular it has determinant 0, a contradiction. □

7 BCH codes

7.1 Digression on finite fields

Here's a fact which you may or may not have seen

Fact 13. *For any prime power* p^k, *there exists a unique field* $\mathbb{F}_{p^k}$ *of order* p^k.

We won't cover the construction in this class[1]. Every finite field $\mathbb{F}_{p^k}$ can be described as follows: let P be an irreducible polynomial of degree k over $\mathbb{F}_p$, then $\mathbb{F}_{p^k} \cong \mathbb{F}_p[x]/(P)$. Essentially, look at all polynomials mod P. This is a field of order p^k.

As an example, we have $\mathbb{F}_4 = F[x]/(x^2 + x + 1)$. In other words, $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$ where α satisfies $\alpha^2 = \alpha + 1$.

Fact 14. *Every field* $\mathbb{F}_{p^k}$ *is naturally a vector space over* $\mathbb{F}_p$ *of dimension* k.

7.2 Motivation and construction of BCH Codes

Reed-Solomon codes optimized the function $R + \delta$ in the limit as $n \to \infty$, but they required us to change our alphabet. We can use the idea behind Reed-Solomon codes to construct optimal codes over $\Sigma = \mathbb{F}_2$. Here optimal is in terms of size - it saturates the volume-packing bound in the limit.

A BCH code is a code of length 2^t over $\mathbb{F}_2$, parametrized by some number $k \leq 2^t - 2$, with distance $2^t - k - 1$. We define them simply as the codewords in RS_k whose image lies in $\mathbb{F}_2 \subset \mathbb{F}_{2^t}$. We can describe our code as follows:

$$C = \{f : \mathbb{F}_{2^t} \to \mathbb{F}_2, \forall i \leq 2^{t-k-2}, \sum_{x \in \mathbb{F}_{2^t}} x^i f(x) = 0\}.$$

As a subset of a Reed-Solomon code, C has distance $2^t - k - 1$. What is the size of C? We'll discuss this next class.

[1] construct a field extension of $\mathbb{F}_p$ over which the polynomial $x^{p^k} - x$ splits and let S be the roots–S is the subfield we want