1 The LP-bound

We will prove the “Linear-Programming bound” due to [2, 1], which gives an upper bound on the code rate of a given distance. The bound’s name hints the proof technique, however we will see a different proof which doesn’t rely on linear programming, due to Navon and Samorodnitsky [3]. The linear-programming bound beats the Elias-Bassalygo bound when the relative distance is not too small.

Before we proceed, consider the notion of a maximal eigenvalue restricted to a specific subset of indices.

Definition 1. Let $A \in \mathbb{C}^{m \times m}$ and $B \subseteq [m]$. Define

$$\lambda_B(A) = \max_{v : \|v\|=1, \text{supp}(v) \subseteq B} v^\dagger Av.$$ 

Throughout, we consider $A$ as the binary adjacency matrix of the Hamming cube of dimension $n$. That is, the rows and column are indexed by $\{0, 1\}^n$ and $A[x, y] = 1$ iff $\Delta(x, y) = 1$ (as $n$-bit strings). Make sure you understand why $\lambda_{\{0, 1\}^n} = n$.

We abbreviate $\lambda_B = \lambda_B(A)$, and note that we can think of every such $v \in \mathbb{R}^{2^n}$ as a function $v : \{0, 1\}^n \rightarrow \mathbb{R}$.

The way we establish an upper bound on the code’s cardinality is by first proving a lower bound on $\lambda_B$ where $B$ is a Hamming ball and then arguing that if a large enough $B$ has a large maximal eigenvalue (w.r.t. the code’s distance) then it must be the case that the code’s cardinality is not too large.

2 The Fourier Transform

We will only consider Fourier expansion over the Boolean cube. Let $V = \{f : \mathbb{F}_2^n \rightarrow \mathbb{R}\}$ and note that it is a vector space on $\mathbb{F}_2^n$ over $\mathbb{R}$ of dimension $2^n$. A natural basis for $V$ is

$$1_w(x) = \begin{cases} 1, & x = w \\ 0, & \text{otherwise} \end{cases}$$

for every $w \in \mathbb{F}_2^n$. It is also an inner-product space under the inner product

$$\langle f_1, f_2 \rangle = \mathbb{E}_{x \in \mathbb{F}_2^n} [f_1(x)f_2(x)] = \frac{1}{2^n} \sum_{x \in G} f_1(x)f_2(x),$$

and it is easy to see that the basis $\{1_w\}_{w \in \mathbb{F}_2^n}$ is an orthogonal basis under this inner product.

We now introduce another basis, that contains only functions that are homomorphisms.
**Definition 2.** A character of the finite group $G$ is a homomorphism $\chi : G \to \mathbb{C}^\times$, i.e., $\chi(x + y) = \chi(x)\chi(y)$ for every $x, y \in G$, where the addition is the group operation in $G$, and the multiplication is the group operation in $\mathbb{C}^\times$.

In our case, $G = \mathbb{F}_2^n$ and we have an explicit representation of the characters. For $S \in \mathbb{F}_2^n$, define $\chi_S \in V$ as

$$\chi_S(x) = (-1)^{(S,x)}.$$ Verify that every character is a homomorphism. Now,

**Claim 3.** The set of all characters of $\mathbb{F}_2^n$ is orthonormal (under the above inner product).

**Proof.** First, $\langle \chi_S, \chi_S \rangle = \frac{1}{2^n} \sum_x \chi_S(x)\chi_S(x) = \frac{1}{2^n} 2^n = 1$. Now, for $S \neq T$,

$$\langle \chi_S, \chi_T \rangle = \frac{1}{2^n} \sum_x \chi_S(x)\chi_T(x) = \frac{1}{2^n} \sum_x (-1)^{(x,S+T)}.$$ As $S \neq T$, $S + T$ is nonzero, say at indices $I \subseteq [n]$. Exactly half of the $x$-s have odd weight restricted to $I$ and exactly half have even weight. Thus, the above sum is 0.  

The **Fourier transform** of a function is the linear transformation from $V$ to $V$ that maps the natural basis to the Fourier basis (of characters). Thus, every $f \in V$ can be (uniquely) written as

$$f = \sum_S \hat{f}(S) \cdot \chi_S,$$

and the coefficients $\hat{f}(S)$ are called the **Fourier coefficients**.

We give their basic properties:

**Claim 4.** Let $f, g \in V$. We have:

1. $\hat{f}(S) = \langle f, \chi_S \rangle$.

2. $\langle f, g \rangle = \sum_S \hat{f}(S)\hat{g}(S)$ (Parseval’s identity).

3. $\hat{f}(\emptyset) = \mathbb{E}[f]$.

**Proof.** For item (1),

$$\langle f, \chi_S \rangle = \left\langle \sum_T \hat{f}(T)\chi_T, \chi_S \right\rangle = \sum_T \hat{f}(T)\langle \chi_S, \chi_T \rangle = \hat{f}(S)\langle \chi_S, \chi_S \rangle = \hat{f}(S).$$

For item (2),

$$\langle f, g \rangle = \left\langle f, \sum_S \hat{g}(S)\chi_S \right\rangle = \sum_S \hat{g}(S)\langle f, \chi_S \rangle = \sum_S \hat{f}(S)\hat{g}(S).$$

For item (3),

$$\hat{f}(\emptyset) = \langle f, \emptyset \rangle = \frac{1}{2^n} \sum_x f(x) \cdot (-1)^0 = \frac{1}{2^n} \sum_x f(x) = \mathbb{E}[f].$$


We now define a convolution between two functions.

**Definition 5.** Let $f, g \in V$. The convolution $f \ast g \in V$ is defined as $(f \ast g)(x) = \mathbb{E}_y f(y)g(x + y)$.

Verify that the convolution operator is commutative and associative. Also, a key property is the following one:

**Claim 6.** $\hat{f} \ast g = \hat{f} \cdot \hat{g}$.

*Proof.* Fix $S \subseteq \mathbb{F}_2^n$. We have:

$$\hat{f}(S) \cdot \hat{g}(S) = \langle f, \chi_S \rangle \langle g, \chi_S \rangle = \frac{1}{2^{2n}} \sum_x \sum_y f(x)g(y)\chi_S(x)\chi_S(y)$$

$$= \frac{1}{2^{2n}} \sum_x \sum_y f(x)g(y)\chi_S(x + y) = \frac{1}{2^{2n}} \sum_x \sum_z f(x)g(z + x)\chi_S(z)$$

$$= \frac{1}{2^n} \sum_z (f \ast g)(z) \cdot \chi_S(z) = \langle f \ast g, \chi_S \rangle = \hat{f} \ast g(S).$$

\[\square\]

### 2.1 Fourier transform and codes

For $C \subseteq \mathbb{F}_2^n$, we let $1_C$ be the characteristic function of $C$, in the sense that $1_C(x) = 1$ if $x \in C$ and 0 otherwise. We record a few easy claims.

**Claim 7.** Let $C$ be a linear code. Then, $\hat{1}_C = \frac{|C|}{2^n} \cdot 1_{C^\perp}$.

*Proof.* For every $S \in \mathbb{F}_2^n$, $\hat{1}_C(S) = \langle 1_C, \chi_S \rangle = \frac{1}{2^n} \sum_x 1_C(x) \cdot (-1)^{(x,S)} = \frac{1}{2^n} \sum_{x \in C} (-1)^{(x,S)}$. Now, if $S \in C^\perp$ then all inner products are 0 and we get $\frac{|C|}{2^n}$.

Otherwise, there exists $c_0 \in C$ such that $\langle c_0, S \rangle = 1$. For every $x \in C$ it holds that $(-1)^{(x,S)} + (-1)^{(x+c_0,S)} = (-1)^{(x,S)}(1 + (-1)^{(c_0,S)}) = 0$. Summing it over all $x \in C$, we get:

$$0 = \sum_{x \in C} ((-1)^{(x,S)}(1 + (-1)^{(x+c_0,S)})) = \sum_{x \in C} (-1)^{(x,S)} + \sum_{x \in C} (-1)^{(x+c_0,S)} = 2 \sum_{x \in C} (-1)^{(x,S)},$$

as required. \[\square\]

**Claim 8.** Let $C$ be a linear code. Then, $1_C \ast 1_C = \frac{|C|}{2^n} \cdot 1_C$.

*Proof.* For every $x \in \mathbb{F}_2^n$, $(1_C \ast 1_C)(x) = \frac{1}{2^n} \sum_y 1_C(y)1_C(x + y) = \frac{1}{2^n} \sum_{y \in C} 1_C(x + y)$. Now, if $x \in C$ then $x + y \in C$ and the sum is $\frac{|C|}{2^n}$. Otherwise, $x + y \notin C$ and the sum is 0. \[\square\]

Let $e_i \in \mathbb{F}_2^n$ be the vector $(a_1, \ldots, a_n)$ with $a_j = \delta_{i,j}$. Let $L : \mathbb{F}_2^n \rightarrow \mathbb{R}$ defined by $L(e_i) = 2^n$ for every $1 \leq i \leq n$, and 0 elsewhere.

**Claim 9.** For every $f \in V$ it holds that $Af = L \ast f$. Consequently, $(Af)(x) = \sum_{i \in [n]} f(x + e_i)$.
Proof. Follows easily by $(f \ast L)(x) = \frac{1}{2^n} \sum_y L(y) f(x + y) = \sum_{i \in [n]} f(x + e_i)$ and inspecting the neighbors of $x$ in the Hamming cube. \hfill \Box

Claim 10. For every $S \in \mathbb{F}_2^n$, $\hat{L}(S) = n - 2 \cdot w(S)$.

Proof. $\hat{L}(S) = \langle L, \chi_S \rangle = \frac{1}{2^n} \sum_x L(x) \cdot (-1)^{\langle x, S \rangle} = \sum_{i \in [n]} (-1)^{S_i} = (n - w(S)) - w(S)$. \hfill \Box

Finally, we give one last example:

Claim 11. Let $B = B(0, \tau n)$ and $C \subseteq \mathbb{F}_2^n$ a code. Then, $(1_C \ast 1_B)(z) = |C \cap B(z, \tau n)|/2^n$.

Proof. For every $z \in \mathbb{F}_2^n$,

$$(1_C \ast 1_B)(z) = \frac{1}{2^n} \sum_x 1_C(x) 1_B(x + z) = \frac{1}{2^n} \sum_{x \in C} 1_B(z, \tau n)(x).$$ \hfill \Box

3 The approach

We say $f \geq g$ if $f(x) \geq g(x)$ for every $x \in \mathbb{F}_2^n$.

Lemma 12. Let $B = B(0, r = \tau n)$ be the Hamming ball of radius $r$. Then there exists a function $f \in V$ with the following properties:

- $f$ is supported on $B$,
- $f \geq 0$,
- $Af \geq \lambda_r f$ for $\lambda_r = 2\sqrt{r(n - r)} - o(n) = 2\sqrt{\tau(1 - \tau)} - o(1))$.

Definition 13. We say $C' \subseteq \mathbb{F}_2^n$ has dual distance $d$ if the Fourier transform of $1_{C'}$ vanishes on points of Hamming weight $0 < |S| < d$.

Claim 14. If $C \subseteq \mathbb{F}_2^n$ is a linear code with dual distance $d$ then $d$ is also the minimal distance of $C^\perp$.

Proof. We want to show that $1_{C^\perp}(x) = 0$ for $x$ with $0 < w(x) < d$. As $C$ is linear, $1_{C^\perp} = \frac{2^n}{|C|} \hat{1}_C$, and by definition $\hat{1}_C(x)$ vanishes on such $x$-s. \hfill \Box

Lemma 15. Suppose $C' \subseteq \mathbb{F}_2^n$ is a vector space with dual distance $d$ (i.e., it’s dual code has distance at least $d$). Let $B = B_r$ for an integer $r$ such that $\lambda_r \geq n - 2d + 1$. Then,

$$\left| \bigcup_{z \in C'} (z + B_r) \right| \geq \frac{2^n}{n}.$$
Let $\delta = d/n < \frac{1}{2}$, take $\tau = \frac{1}{2} - \sqrt{\delta(1-\delta)} + o(1)$ and $r = \tau n$. So,

$$\lambda_r = 2n \left( \sqrt{\left( \frac{1}{2} - \sqrt{\delta(1-\delta)} + o(1) \right)} \left( \frac{1}{2} + \sqrt{\delta(1-\delta)} + o(1) \right) - o(1) \right)$$

$$= 2n \left( \sqrt{\delta^2 - \delta + \frac{1}{4} + o(1)} - o(1) \right) = 2n \left( \frac{1}{2} \sqrt{4\delta^2 - 4\delta + 1} + o(1) \right)$$

$$= 2n \left( \frac{1}{2} (1 - 2\delta) + o(1) \right) = n - 2d + o_n(1) \geq n - 2d + 1,$$

and the premise of Lemma 15 is satisfied by choosing the $o(1)$ terms both in $\lambda_r$ and in $\tau$ appropriately. From now on, that is the $r$ we should think of.

Now take $C' = C^\perp$. Then, balls of radius $r$ centered at the points of the dual code cover an $\frac{1}{n}$-fraction of the space. Then,

$$|C^\perp| \cdot |B_r| = |C^\perp| \cdot 2^n (H(\tau) + o(1)) \geq \frac{2^n}{n},$$

and so we obtain:

**Corollary 16.** Let $C$ be a $[n,k,d]_2$ code and $\delta = d/n$ is the relative distance. Then:

$$|C^\perp| \geq 2^{(1 - H(\tau) - o(1))n}$$

and therefore

$$|C| = \frac{2^n}{|C^\perp|} \leq 2^{(H(\tau) + o(1))n},$$

where $\tau = \frac{1}{2} - \sqrt{\delta(1-\delta)}$.

Asymptotically, this gives $R(\delta) \leq H\left(\frac{1}{2} - \sqrt{\delta(1-\delta)}\right)$. We are left with proving Lemma 12 and Lemma 15.

### 3.1 Proving a lower bound on the Dirichlet eigenvalue of a ball in $\mathbb{F}_2^n$

**Lemma 17.** Let $B = B(0,r = \tau n)$ be the Hamming ball of radius $r$. Then there exists a function $f \in V$ with the following properties:

- $f$ is supported on $B$,
- $f \geq 0$,
- $\langle Af, f \rangle \geq \lambda_r \langle f, f \rangle$ for $\lambda_r = 2 \sqrt{r(n-r)} - o(n) = 2n (\sqrt{\tau(1-\tau)} - o(1))$.

**Proof.** We construct a specific “eigenfunction” $f$ that achieves the bound. $f$ will be symmetric, so it is fully defined by its values on $n+1$ vectors of distinct Hamming weights. We overload notation and write $f(i)$ for the value given on weight $i$ vectors. We choose $f$ such that $f$ gives the same weight for each level on its support. Let $M = \sqrt{n} = o(n)$. Define $f$ as follows:

$$f(i) = \begin{cases} 
\frac{1}{\sqrt{\binom{n}{i}}} & i \in [r-M, r], \\
0 & \text{otherwise}.
\end{cases}$$
Now we need to compute \((Af)(v) = \sum_{j=1}^{n} f(v + e_j)\). Notice that \(Af\) is also symmetric and
\[
Af(i) = if(i - 1) + (n - i)f(i + 1).
\]
Also, if \(i \in [r - M, r - 1]\),
\[
\frac{f(i)}{f(i + 1)} = \sqrt{\frac{n}{i+1}} = \sqrt{\frac{n-i}{i+1}}.
\]
Thus, for \(i \in [r - M + 1, r - 1]\),
\[
Af(i) = \sqrt{i(n-i)} f(i) + \sqrt{(n-i)(i+1)} f(i).
\]
Hence,
\[
f^\dagger Af \geq \sum_{k=r-M+1}^{r-1} \binom{n}{k} \cdot (\sqrt{k(n-k+1)} + \sqrt{(n-k)(k+1)}) f(k)^2
\]
\[
= \sum_{k=r-M+1}^{r-1} \sqrt{k(n-k+1)} + \sqrt{(n-k)(k+1)}.
\]
As
\[
\sqrt{k(n-k+1)}, \sqrt{(n-k)(k+1)} \geq \sqrt{(r-M)(n-r)} \geq \sqrt{r(n-r) - M},
\]
we get that
\[
f^\dagger Af \geq 2(M-1)(\sqrt{r(n-r)} - M) = 2\sqrt{r(n-r)} - o(n),
\]
whereas \(f^\dagger f \leq 1\), completing the proof.

Having that we prove Lemma 12

**Proof.** \(A\) is a symmetric, irreducible (i.e., the corresponding graph is connected) operator with non-negative entries. Let \(A'\) be its restriction to \(B\) (one can view it as either restricting the matrix \(A\) to the \(B \times B\) sub-rectangle, or as the operator \(\Pi_B A \Pi_B\) where \(\Pi_B\) is projection on \(B\)). \(A'\) is also symmetric, irreducible and with non-negative entries. By the Perron-Frobenius theorem the greatest eigenvalue of \(A'\) is obtained by a non-negative vector \(f' \geq 0\) supported on \(B\). Say \(A'^\dagger f' = \lambda' f'\).

We have already seen an \(f\) supported on \(B\) such that \(\frac{f^\dagger Af}{f^\dagger f} \geq \lambda_r\). However, \(f^\dagger Af = f^\dagger \Pi_B A \Pi_B f = f'^\dagger A' f\), and \(\lambda'\) is the largest singular value of \(A'\), hence we must have \(\lambda' \geq \lambda_r\). Also \(Af' \geq A'f'\) because \(A - A' \geq 0\) and \(f' \geq 0\), hence we have
\[
Af' \geq A'f' \geq \lambda' f' \geq \lambda f',
\]
as desired.
3.2 The covering bound

Proof. Let $B = B_r$ and $f$ be the function guaranteed by Lemma 12 for $B$. Define

$$F = 1_{C'} * f.$$ 

I.e., for $z \in \mathbb{F}_2^n$:

$$F(z) = \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} 1_{C'}(x) f(x + z) = \frac{1}{2^n} \sum_{w \in C'} f(z + w).$$

Hence, $F$ is supported on $\bigcup_{w \in C'} (w + B)$. We will bound $\langle AF, F \rangle$ from both sides.

**One side:** By definition,

$$AF = F * L = (1_{C'} * f) * L = 1_{C'} * (f * L) = 1_{C'} * Af.$$ 

As $1_{C'} \geq 0$ and $Af \geq \lambda_B f$ we have $AF = 1_{C'} * Af \geq \lambda_B 1_{C'} * f = \lambda_B F$. Thus,

$$\langle AF, F \rangle \geq \lambda_B \langle F, F \rangle.$$ 

**Other side:** It holds that

$$\langle AF, F \rangle = \sum_{S} \hat{AF}(S) \hat{F}(S) = \sum_{S} \hat{L} \ast \hat{F}(S) \hat{F}(S) = \sum_{S} \hat{L}(S) \hat{F}(S) \hat{F}(S).$$

But $\hat{F}(S) = \hat{1}_{C'} * \hat{f}(S) = \hat{1}_{C'}(S) \hat{f}(S)$, and $C'$ has dual distance $d$, so we get zero for every set $S$ of cardinality between $1$ and $d - 1$. Hence,

$$\langle AF, F \rangle = \hat{L}(\emptyset)(\hat{F}(\emptyset))^2 + \sum_{S:w(S) \geq d} \hat{L}(S)(\hat{F}(S))^2$$

$$= n(\hat{F}(\emptyset))^2 + \sum_{S:w(S) \geq d} (n - 2w(S))(\hat{F}(S))^2$$

$$\leq n(\hat{F}(\emptyset))^2 + \sum_{S} (n - 2d)(\hat{F}(S))^2.$$ 

Together we get that

$$(n - 2d + 1)\langle F, F \rangle \leq \lambda_B \langle F, F \rangle \leq \langle AF, F \rangle \leq n \mathbb{E}[F]^2 + (n - 2d)\langle F, F \rangle.$$

Thus,

$$\langle F, F \rangle \leq n \mathbb{E}[F]^2.$$ 

But, $F$ is supported on $\Lambda = \bigcup_{w \in C'} (w + B)$, and by Cauchy-Schwartz,

$$\mathbb{E}[F]^2 = \left( \frac{1}{2^n} \sum_{x \in \Lambda} 1 \cdot F(x) \right)^2 \leq \frac{1}{2^{2n}} |\Lambda| \cdot \sum_{x} F^2(x) = \frac{|\Lambda|}{2^n} \langle F, F \rangle$$

Hence $1 \leq \frac{n|\Lambda|}{2^n}$, as desired. \qed
References

