CS 860 Topics in Coding Theory September 22, 2025

Lecture 4+5

Lecturer: Elena Grigorescu *Scribe: Zhiang Wu*

In this note, we use $\langle \cdot, \cdot \rangle$ to denote the inner product. Let $[n] = \{1, 2, \ldots, n\}$.

1 Hadamard Code

Last time, we ended with the Plotkin bound as follows.

Claim 1 (Plotkin bound) *Let $C \subseteq \mathbb{F}_2^n$ denote a binary code of code length n and distance d. If $d \geq \frac{n}{2}$, then $|C| \leq 2n$.*

When $d = \frac{n}{2}$, we will see that the *Hadamard code* achieves the tight size bound. Below, we first define the Hadamard code and introduce the notion of *dual code*. Next, we demonstrate that the Hadamard code is the dual of the Hamming code. Finally, we show the distance and size of the Hadamard code.

Definition 2 (Hadamard Code) *Recall that the Hamming code* Ham *is*

$$\mathrm{Ham} = \left\{ c \in \mathbb{F}_2^{2^t-1} \mid Hc = 0 \bmod 2 \right\},$$

where $H \in \mathbb{F}_2^{t \times (2^t-1)}$ and the i-th column of H is the binary representation of i.

The Hadamard code Had *is defined with respect to H as*

$$\mathrm{Had} = \left\{ c \in \mathbb{F}_2^{2^t-1} \mid a^\top H = c \text{ for some } a \in \mathbb{F}_2^t \right\}.$$

We observe the following property of the Hadamard code.

Claim 3 (Property of Had**)** $\forall\ c \in \mathrm{Had}$*,* $\forall y \in \mathrm{Ham}$*,* $\langle c, y \rangle = 0$.

Proof By the definition of Had, since $c \in \mathrm{Had}$, there exists $a \in \mathbb{F}_2^t$ such that $a^\top H = c$. Then $\langle c, y \rangle = \left\langle a^\top H, y \right\rangle = \langle a, Hy \rangle$. Since $y \in \mathrm{Ham}$, then $Hy = 0$. Hence $\langle c, y \rangle = 0$. ■

Definition 4 (Dual Code) *For a linear code $C \subseteq \mathbb{F}_2^n$, its dual code, denoted as $C^\perp$, is*

$$C^\perp = \left\{ c' \in \mathbb{F}_2^n \mid \left\langle c', c \right\rangle = 0\ \forall c \in C \right\}.$$

Remark Had is the dual code of Ham.

Claim 5 (Size of Had**)** *Let* $n = 2^t - 1$. *Then* $|\mathrm{Had}| = n + 1$.

Proof From lecture 2, we have $\dim(\mathrm{Ham}) = \dim(\ker(H)) = n - t$. Note that Had is the orthogonal complement of Ham. Then $\dim(\mathrm{Had}) = t$ by the fundamental theorem of linear algebra. Hence, $|\mathrm{Had}| = 2^t = n + 1$. ■

Before proving the distance of Had, we discuss an alternative view of the Hadamard code. Each codeword c is considered as a function parameterized by $a \in \mathbb{F}_2^t$, i.e.,

$$\mathrm{Had} = \{c_a : \mathbb{F}_2^t \backslash \{0\} \to \mathbb{F}_2 \mid a \in \mathbb{F}_2^t\},$$

where $c_a(x) = \langle a, x \rangle$ for $x \in \mathbb{F}_2^t \backslash \{0\}$. For each codeword $c \in \mathrm{Had}$, it can be represented as $c = (\langle a, b_1 \rangle, \ldots, \langle a, b_{2^t-1} \rangle)$, where $b_i \in \mathbb{F}_2^t$ corresponds to the binary representation of i for $i \in [2^t - 1]$.

Claim 6 (Distance of Had**)** *Let* $n = 2^t - 1$. *Then* $\Delta(\mathrm{Had}) = \frac{n+1}{2}$.

Proof From lecture 2, it is equivalent to show that $\min_{\substack{c \in \mathrm{Had} \\ c \neq 0}} wt(c, 0) = \frac{n+1}{2}$. We prove that for every $x \in \mathbb{F}_2^t \backslash \{0\}$ such that $\langle a, x \rangle = 0$, we can uniquely pair x with $x' \in \mathbb{F}_2^t \backslash \{0, x\}$ so that $c_a(x') = 1$. Let $x' = x + e_j$, where $a_j \neq 0$ and e_j is j-th standard basis. Then $\langle a, x + e_j \rangle = \langle a, x \rangle + \langle a, e_j \rangle = a_j = 1$. Since $c \neq 0$, at least one $\langle a, x \rangle \neq = 0$. Hence, the distance of Had is $\frac{2^t-2}{2} + 1 = \frac{n+1}{2}$. ■

We have show that there exists a code Had such that $|\mathrm{Had}| = n + 1$ and $\Delta(\mathrm{Had}) = \frac{n+1}{2}$ for an odd integer n. It can be simply extended to an arbitrary integer by considering the following construction:

$$\mathrm{Had}' = \left\{c_{a,b} : \mathbb{F}_2^t \backslash \{0\} \to \mathbb{F}_2 \mid a \in \mathbb{F}_2^t, b \in \mathbb{F}_2\right\},$$

where $c_{a,b}(x) = \langle a, x \rangle + b$ for $x \in \mathbb{F}_2^t \backslash \{0\}$.

2 Fourier Analysis over the Boolean Hypercube

We consider the vector space of real-valued functions over the boolean hypercube, i.e., $V = \{f : \mathbb{F}_2^n \to \mathbb{R}\}$. There are two basis. The first is the standard basis $\{\mathbb{1}_w \mid w \in \mathbb{F}_2^n\}$, where

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

The second is the *Fourier basis* $\{\chi_y : \mathbb{F}_2^n \to \mathbb{R} \mid y \in \mathbb{F}_2^n\}$, where $\chi_y(x) = (-1)^{\langle x, y \rangle}$ for $x \in \mathbb{F}_2^n$. We make the following two observations:

- $\forall x, z \in \mathbb{F}_2^n$, $\chi_y(x)\chi_y(z) = \chi_y(x + z)$;
- $\forall x, z \in \mathbb{F}_2^n$, $\chi_x(y)\chi_z(y) = \chi_{x+z}(y)$.

Recall that the inner product $\langle\cdot,\cdot\rangle : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{R}$ of two functions $f, g : \mathbb{F}_2^n \to \mathbb{R}$ is

$$\langle f, g\rangle = \mathbb{E}[fg] = \sum_{x\in\mathbb{F}_2^n} \frac{1}{2^n} f(x)g(x).$$

Claim 7 *The Fourier basis is an orthonormal basis.*

Proof **Norm of χ_y.** For each χ_y, we have $\langle \chi_y, \chi_y\rangle = \frac{1}{2^n}\sum_x \chi_y(x+x) = \frac{1}{2^n}\sum_x (-1)^0 = 1$. **Orthogonal.** For $\chi_y \neq \chi_z$, we have $\langle \chi_y, \chi_z\rangle = \frac{1}{2^n}\sum_x \chi_{y+z}(x) = \frac{1}{2^n}\sum_x (-1)^{\langle y+z,x\rangle}$. Note that $y+z \neq 0$. We apply the same trick used in Claim 6 to pair each x where $\langle y+z, x\rangle = 0$ to a unique x' such that $\langle y+z, x'\rangle = 1$. We have $(-1)^{\langle y+z,x\rangle} + (-1)^{\langle y+z,x'\rangle} = 0$. Hence, $\langle \chi_y, \chi_z\rangle = 0$. ∎

Definition 8 (Fourier Transform) *For a function $f \in V$, it can be uniquely expressed as*

$$f = \sum_{y\in\mathbb{F}_2^n} \hat{f}(y)\chi_y,$$

where $\hat{f} : \mathbb{F}_2^n \to \mathbb{R}$.

Claim 9 $\forall y \in \mathbb{F}_2^n$, $\hat{f}(y) = \langle f, \chi_y\rangle$.

Proof

$$\begin{aligned}
\langle f, \chi_y\rangle &= \left\langle \sum_x \hat{f}(x)\chi_x, \chi_y \right\rangle \\
&= \sum_x \hat{f}(x)\langle \chi_x, \chi_y\rangle \\
&= \hat{f}(y)\langle \chi_y, \chi_y\rangle + \sum_{x\in\mathbb{F}_2^n : x\neq y} \hat{f}(x)\langle \chi_x, \chi_y\rangle \\
&= \hat{f}(y) + 0,
\end{aligned}$$

where the first equality follows from Definition 8, and the forth inequality follows from Claim 7. ∎

Claim 10 (Parseval's Identity) $\forall f, g \in V$, $\langle f, g\rangle = \sum_y \hat{f}(y)\hat{g}(y)$.

Proof

$$\langle f, g\rangle = \left\langle f, \sum_y \hat{g}(y)\chi_y \right\rangle = \sum_y \hat{g}(y)\langle f, \chi_y\rangle = \sum_y \hat{g}(y)\hat{f}(y),$$

where the first equality follows from Definition 8, and the second equality follows form Claim 9. ∎

Corollary 11 $\forall f \in V,\ \hat{f}(0) = \mathbb{E}[f]$.

Proof

$$\hat{f}(0) = \langle f, \chi_0 \rangle = \mathbb{E}[f],$$

where the first equality follows form Claim 9, and the second equality follows form $\chi_0 = 1$. ■

Definition 12 (Convolution) *$\forall f, g \in V$, the convolution of f and g is*

$$(f * g)(x) = \mathbb{E}_y[f(y)g(x+y)].$$

Claim 13 *The convolution operator $*$ is commutative and associative.*

Claim 14 $\forall x \in \mathbb{F}_2^n$, $\widehat{f * g}(x) = \hat{f}(x)\hat{g}(x)$.

Proof

$$\begin{aligned}
\hat{f}(x)\hat{g}(x) &= \langle f, \chi_x \rangle \langle g, \chi_x \rangle \\
&= \frac{1}{2^{2n}} \left(\sum_y f(y)\chi_x(y) \right) \left(\sum_z g(z)\chi_x(z) \right) \\
&= \frac{1}{2^{2n}} \sum_{y,z} f(y)g(z)\chi_x(y+z) \\
&= \frac{1}{2^{2n}} \sum_{y,t} f(y)g(t+y)\chi_x(t) \\
&= \frac{1}{2^n} \sum_t \chi_x(t) \left(\sum_y \frac{1}{2^n} f(y)g(t+y) \right) \\
&= \frac{1}{2^n} \sum_t \chi_x(t)(f * g)(t) \\
&= \langle \chi_x, f * g \rangle \\
&= \widehat{f * g}(x),
\end{aligned}$$

where the first and last equalities follow from Claim 9. ■

For a code $C \subseteq \mathbb{F}_2^n$, define its characteristic functions as

$$\mathbb{1}_C(c) = \begin{cases} 1 & \text{if } c \in C \\ 0 & \text{otherwise} \end{cases}.$$

3 Application of Fourier Analysis

Claim 15 *Let $C \subseteq \mathbb{F}_2^n$ be a linear code. Then $\widehat{\mathbb{1}_C} = \frac{|C|}{2^n}\mathbb{1}_{C^\perp}$.*

Proof $\forall x \in \mathbb{F}_2^n$,

$$
\begin{aligned}
\widehat{\mathbb{1}_C}(x) &= \left\langle \widehat{\mathbb{1}_C}, \chi_x \right\rangle \\
&= \frac{1}{2^n}\sum_y \widehat{\mathbb{1}_C}(y)\chi_x(y) \\
&= \frac{1}{2^n}\left(\sum_{y\in\mathbb{F}_2^n: y\in C} \widehat{\mathbb{1}_C}(y)\chi_x(y) + \sum_{y\in\mathbb{F}_2^n: y\notin C} \widehat{\mathbb{1}_C}(y)\chi_x(y)\right) \\
&= \frac{1}{2^n}\sum_{y\in\mathbb{F}_2^n: y\in C} \chi_x(y) \\
&= \frac{1}{2^n}\sum_{y\in\mathbb{F}_2^n: y\in C} (-1)^{\langle x,y\rangle},
\end{aligned}
$$

where the forth equality follows from the definition of $\widehat{\mathbb{1}_C}$. Note that if $x \in C^\perp$, $\langle x, y\rangle = 0$ and $\sum_{y\in\mathbb{F}_2^n: y\in C}(-1)^{\langle x,y\rangle} = |C|$. Otherwise, there exists $y^* \in \mathbb{F}_2^n$ such that $\langle x, y^*\rangle = 1$. By the same trick used in Claim 6, if $x \notin C^\perp$, we have $\sum_{y\in\mathbb{F}_2^n: y\in C}(-1)^{\langle x,y\rangle} = 0$. ■

Claim 16 *Let $C \subseteq \mathbb{F}_2^n$. Then $\mathbb{1}_C * \mathbb{1}_C = \frac{|C|}{2^n}\mathbb{1}_C$.*

Proof $\forall x \in \mathbb{F}_2^n$,

$$
\begin{aligned}
(\mathbb{1}_C * \mathbb{1}_C)(x) &= \sum_y \left(\widehat{\mathbb{1}_C * \mathbb{1}_C}(y)\right)\chi_y(x) \\
&= \left(\frac{|C|}{2^n}\right)^2 \sum_y \left(\mathbb{1}_{C\perp}(y)\right)\chi_y(x) \\
&= \left(\frac{|C|}{2^n}\right)^2 \sum_{y\in\mathbb{F}_2^n: y\in C^\perp} \chi_y(x).
\end{aligned}
$$

Since C is linear, we have $|C^\perp| \cdot |C| = 2^n$. By the same tricks used in Claim 6 and Claim 14, we have

$$
\left(\frac{|C|}{2^n}\right)^2 \sum_{y\in\mathbb{F}_2^n: y\in C^\perp} \chi_y(x) = \left(\frac{|C|}{2^n}\right)^2 |C^\perp|\mathbb{1}_C = \frac{|C|}{2^n}\mathbb{1}_C.
$$

■

4 LP Bound

The goal of this section is to prove the following theorem.

Theorem 17 (LP Bound) *Let $C \subseteq \mathbb{F}_2^n$ be a linear code of distance $d \leq \frac{n}{2}$ and $\delta = \frac{d}{n}$. Then*

$$|C| \leq 2^{(H(\tau_{\mathrm{LP}})+o(1))n},$$

where $\tau_{\mathrm{LP}} = \frac{1}{2} - \sqrt{\delta(1-\delta)}$.

Below, we first state the covering lemma and directly apply it to derive the LP bound. Then, we prove the covering lemma via a helper lemma on the existence of a function of special properties. Finally, we introduce the special function to end the proof.

We define $r = \tau n$ as a function of τ and $\theta_r = 2\sqrt{r(1-r)} - o(n)$ as a function of r.

Lemma 18 (Covering Lemma) *Let $C \subseteq \mathbb{F}_2^n$ be a linear code of distance d and $C^\perp$ be the dual of C. Let r be a radius such that $\theta_r \geq n - 2d + 1$ and B_r be the hamming bal of radius r, where $r = \tau n$ and $\theta_r = 2\sqrt{r(n-r)} - o(n) = 2n(\sqrt{\tau(1-\tau)} - o(1))$. Then*

$$\left| \bigcup_{z \in C^\perp} (z + B_r) \right| \geq \frac{2^n}{n}.$$

4.1 Proof of the LP Bound

Proof Now, we leverage the covering lemma to prove LP bound. Take $r = \tau_{\mathrm{LP}} n$. We neglect the $o(1)$ terms and verify that $\theta_r \geq n - 2d + 1$ below.

$$\begin{aligned}
\theta_r &= 2n\sqrt{\tau_{\mathrm{LP}}(1-\tau_{\mathrm{LP}})} \\
&= 2n\sqrt{\left(\frac{1}{2} - \sqrt{\delta(1-\delta)}\right)\left(\frac{1}{2} + \sqrt{\delta(1-\delta)}\right)} \\
&= 2n\sqrt{\delta^2 - \delta + \frac{1}{4}} \\
&\geq n - 2d + 1.
\end{aligned}$$

Note that

$$\left| \bigcup_{z \in C^\perp} (z + B_r) \right| \leq \sum_{z \in C^\perp} |z + B_r| = |C^\perp| \cdot |B_r| = \frac{2^n}{|C|} 2^{(H(\tau_{\mathrm{LP}})+o(1))n},$$

since $|C^\perp| \cdot |C| = 2^n$ and $|B_r| = 2^{(H(\tau_{\mathrm{LP}})+o(1))n}$. Meanwhile, the covering lemma (Lemma 18) gives a lower bound of $\left|\bigcup_{z \in C^\perp}(z + B_r)\right|$. Then

$$\frac{2^n}{n} \leq \left| \bigcup_{z \in C^\perp} (z + B_r) \right| \leq \frac{2^n}{|C|} 2^{(H(\tau_{\mathrm{LP}})+o(1))n}.$$

We have $|C| \leq n 2^{(H(\tau_{\mathrm{LP}})+o(1))n} = 2^{(H(\tau_{\mathrm{LP}})+o(1))n}$ as n is absorbed by the $o(1)$ term. ■

4.2 Proving the Covering Lemma

Below, we first set up useful notations and observations. Then, we state a helper lemma and apply it to derive the covering lemma. Finally, we prove the helper lemma.

For two functions f and g, we denote $f \geq g$ if and only if $f(x) \geq g(x)$ for any x.

We consider a layered graph based on the boolean hypercube $\mathbb{F}_2^n$. There is an edge between $v_i, v_j \in \mathbb{F}_2^n$ if and only if $\Delta(v_i, v_j) = 1$, i.e., $v_i = v_j + e_k$ for some $k \in [n]$, where $e_k \in \mathbb{F}_2^n$ is the k-th standard basis of $\mathbb{F}_2^n$. Let A denote the adjacency matrix of the layer graph. Then $A_{y,y+e_k} = 1$ for each $y \in \mathbb{F}_2^n$ such that $y \neq 1$, and each $k \in [n]$.

Consider the function $L : \mathbb{F}_2^n \to \mathbb{R}$ defined as follows.

$$L(x) = \begin{cases} 2^n & \text{if } x = e_k \text{ for some } k \in [n] \\ 0 & \text{otherwise} \end{cases}.$$

Claim 19 *$\forall f \in V$, $Af = L * f$.*

Proof $\forall x \in \mathbb{F}_2^n$, $(L * f)(x) = \sum_y \frac{1}{2^n} L(y) f(y + x)$. Note that $L(y) = 2^n$ if and only if $y = e_k$ for some $k \in [n]$. Then $(L * f)(x) = \sum_{i \in [n]} f(x + e_i)$, which is exactly the definition of $(Af)(x)$ since $A_{x,x'} = 1$ if $x' = x + e_k$ for some $k \in [n]$. ■

Claim 20 *$\forall x \in \mathbb{F}_2^n$, $\hat{L}(x) = n - 2\mathrm{wt}(x)$.*

Proof

$$\begin{aligned}
\hat{L}(x) &= \langle L, \chi_x \rangle \\
&= \frac{1}{2^n} \sum_z (-1)^{\langle z,x \rangle} L(z) \\
&= \frac{1}{2^n} \sum_{i \in [n]} (-1)^{\langle e_i,x \rangle} L(e_i) \\
&= \sum_{i \in [n]} (-1)^{x_i} \\
&= |\{i \in [n] \mid x_i = 0\}| - |\{i \in [n] \mid x_i = 1\}| = n - 2\mathrm{wt}(x).
\end{aligned}$$

■

Claim 21 *Let $B = B(0, \tau n)$. Let $C \subseteq \mathbb{F}_2^n$ be a code. $\forall x \in \mathbb{F}_2^n$, $(\mathbb{1}_C * \mathbb{1}_B)(x) = \frac{|C \cap B(x,\tau n)|}{2^n}$.*

Proof

$$\begin{aligned}
(\mathbb{1}_C * \mathbb{1}_B)(x) &= \frac{1}{2^n} \sum_y \mathbb{1}_C(y) \mathbb{1}_B(x + y) \\
&= \frac{1}{2^n} \sum_{y \in C} \mathbb{1}_B(x + y).
\end{aligned}$$

Note that $\mathbb{1}_B(x+y) = 1$ if $x + y \in B$, i.e., $y \in B(x, \tau n)$. Hence, $(\mathbb{1}_C * \mathbb{1}_B)(x) = \frac{|C \cap B(x,\tau n)|}{2^n}$.
■

Lemma 22 (Helper Lemma) *Let $r = \tau n$. Let $B = B(0, r)$ denote the Hamming ball of radius r. There exists a function $\mathsf{f} : \mathbb{F}_2^n \to \mathbb{R}$ such that*

(1) $\mathrm{supp}(\mathsf{f}) \subseteq B$*;*

(2) $\mathsf{f} \geq 0$*;*

(3) $A\mathsf{f} \geq \theta_r \mathsf{f}$*, where* $\theta_r = 2\sqrt{r(n-r)} - o(n)$*.*

Remark The helper lemma implies that the largest eigenvalue of A is at least θ_r.

$$\lambda_B = \max \left\{ \frac{\langle Af, f \rangle}{\langle f, f \rangle} \;\middle|\; f :\in \mathbb{F}_2^n \to \mathbb{R},\ \mathrm{supp}(f) \subseteq B \right\} \geq \theta_r.$$

Now, we are ready to prove the covering lemma.

Proof of the Covering Lemma Let f denote a function given by the helper lemma. Consider a function $F : \mathbb{F}_2^n \to \mathbb{R}$ defined as follows:

$$F(z) = \left(\mathbb{1}_{C^\perp} * \mathsf{f}\right)(z) = \frac{1}{2^n} \sum_x \mathbb{1}_{C^\perp}(x)\mathsf{f}(x+z). \tag{1}$$

Note that $F(z) \neq 0$ only if there exits some $x \in C^\perp$ such that $\mathsf{f}(x+z) \neq 0$. Then $x + z \in B$, i.e., $x \in z + B$, since $\mathrm{supp}(\mathsf{f}) \subseteq B$. Hence, $\mathrm{supp}(F) \subseteq S$, where $S = \bigcup_{z \in C^\perp}(z + B)$.

We next consider the expectation of F to relate $|S|$.

$$\begin{aligned}
(\mathbb{E}[F])^2 &= \left(\frac{1}{2^n} \sum_{x \in S} F(x) \right)^2 \\
&\leq \frac{1}{2^{2n}} |S| \left(\sum_{x \in S} F^2(x) \right) \\
&= \frac{|S|}{2^n} \langle F, F \rangle \\
&\leq \frac{|S|}{2^n} n (\mathbb{E}[F])^2,
\end{aligned}$$

where the first inequality follows from the Cauchy-Schwartz inequality, the second equality follows from the definition of inner product, and the second inequality follows from Claim 23.

Hence, $|S| \geq \frac{2^n}{n}$. ■

Claim 23 *For the function $F \in V$ defined as Equation (1), $\langle F, F\rangle \le n(\mathbb{E}[F])^2$*

Proof We consider the upper and lower bounds of $\langle AF, F\rangle$.
Lower Bound. We have

$$\begin{aligned} AF &= F * L \\ &= (\mathbb{1}_{C^\perp} * \mathsf{f}) * L \\ &= \mathbb{1}_{C^\perp} * (\mathsf{f} * L) \\ &= \mathbb{1}_{C^\perp} * A\mathsf{f} \\ &\ge \mathbb{1}_{C^\perp} * \theta_r \mathsf{f} \\ &= \theta_r(\mathbb{1}_{C^\perp} * \mathsf{f}) \\ &= \theta_r F, \end{aligned}$$

where the equalities follows from the definitions of F and convolution, and the inequality follows from the helper lemma. Then $\langle AF, F\rangle \ge \theta_r\langle F, F\rangle \ge (n-2d+1)\langle F, F\rangle$.
Upper Bound. We have

$$\langle AF, F\rangle = \sum_x \widehat{AF}(x)\hat{F}(x) = \sum_x \widehat{L * F}(x)\hat{F}(x) = \sum_x \hat{L}(x)\hat{F}(x)\hat{F}(x).$$

Recall that $F(x) = (\mathbb{1}_{C^\perp} * \mathsf{f})(x)$ and $\hat{F}(x) = \widehat{\mathbb{1}_{C^\perp} * \mathsf{f}}(x) = \widehat{\mathbb{1}_{C^\perp}}(x)\hat{\mathsf{f}}(x) = \frac{|C|}{2^n}\mathbb{1}_C(x)\hat{\mathsf{f}}(x)$. Then $\hat{F}(x) = 0$ for any $x \in \mathbb{F}_2^n$ such that $1 \le \mathrm{wt}(x) \le d-1$, since C is of distance d.

$$\begin{aligned} \sum_x \hat{L}(x)\hat{F}(x)\hat{F}(x) &= \hat{L}(0)\hat{F}^2(0) + \sum_{x\in\mathbb{F}_2^n:\mathrm{wt}(x)\ge d} \hat{L}(x)\hat{F}^2(x) \\ &= \mathbb{E}[L](\mathbb{E}[F])^2 + \sum_{x\in\mathbb{F}_2^n:\mathrm{wt}(x)\ge d} (n - 2\mathrm{wt}(x))\hat{F}^2(x) \\ &\le n(\mathbb{E}[F])^2 + (n-2d)\langle F, F\rangle. \end{aligned}$$

Combing the upper and lower bounds, we have

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

Hence, $\langle F, F\rangle \le n(\mathbb{E}[F])^2$. ■

Finally, we construct a special function for the helper lemma.

Proof of the Helper Lemma We consider the function constructed as follows. First, we let $\mathsf{f}(x) = \mathsf{f}(y)$ if $x, y \in \mathbb{F}_2^n$ such that $\mathrm{wt}(x) = \mathrm{wt}(y)$. We abuse the notation and denote $\mathsf{f}(i)$ as the values of weight i vectors in $\mathbb{F}_2^n$. Recall that $r = \tau n$.

$$\mathsf{f}(i) = \begin{cases} \frac{1}{\sqrt{\binom{n}{i}}} & \text{if } i \in [r - \sqrt{n}, r] \\ 0 & \text{otherwise} \end{cases}.$$

It is easy to see that $\mathrm{supp}(\mathsf{f}) \subseteq B$ and $\mathsf{f} \ge 0$. Below, we verify that $A\mathsf{f} \ge \theta_r\mathsf{f}$.

Recall that $A\mathsf{f}(x) = \sum_{i \in [n]} \mathsf{f}(x + e_i)$. Then

$$A\mathsf{f}(x) = \mathrm{wt}(x)\mathsf{f}(\mathrm{wt}(x) - 1) + (n - \mathrm{wt}(x))\mathsf{f}(\mathrm{wt}(x) + 1),$$

since there are $\mathrm{wt}(x)$ vectors of weight $\mathrm{wt}(x) - 1$ from x. Thus, for $i \in [r - \sqrt{n} + 1, r - 1]$,

$$A\mathsf{f}(i) = \left(\sqrt{i(n-i)} + \sqrt{(n-i)(i+1)}\right)\mathsf{f}(i) \geq \left(2\sqrt{r(n-r)} - o(n)\right)\mathsf{f}(i),$$

where the equality follows from the construction of f and $\frac{\mathsf{f}(i)}{\mathsf{f}(i+1)} = \sqrt{\frac{\binom{n}{i+1}}{\binom{n}{i}}} = \sqrt{\frac{n-i}{i+1}}$. ■