APM461 Lecture Notes

Arky!! :3c

'25 Winter Semester

Contents

§1 Day 1: Hall's Theorem (Jan. 8, 2025)

The course textbook is Van Lint and Wilson, link here. The grading scheme is given by

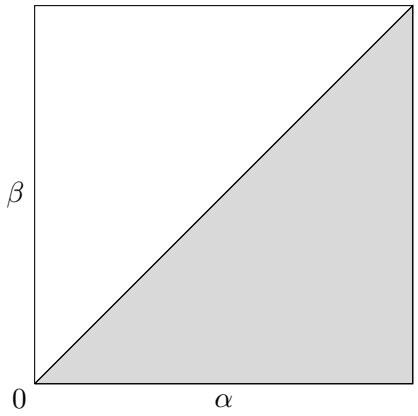
(i) 30% Scribing: i.e., writing out the lecture notes on LaTeX;

(ii) 30% Homeworks;

(iii) 40% Final Exam.

The knowledge prerequisites for this class are linear algebra, basic discrete probability, and simple combinatorics. This class is about combinatorial and discrete objects, and extremal problems about them.

As an example, consider $[n] = \{1, \dots, n\}$, and $\alpha \geq \beta \in [0, 1]$. We want $A_1, \dots A_k \subseteq [n]$ such that $|A_i| \geq \alpha n$ for all i, with $|A_i \cap A_j| \leq \beta n$. How big can k be? What are the asymptotics as $n \to \infty$ if we leave α, β fixed? Consider the following square, where the



gray triangle represents the possible choices of α, β.[1] We may note that

$$k \geq \binom{n}{\frac{n}{2}} \approx O\left(\frac{2^n}{\sqrt{n}}\right).$$

We now work to introduce Hall's Theorem. Consider a bipartite graph, with n vertices on both sides (where we will let $V = L \sqcup R$), and the edge set $E \subseteq L \times R$.

Definition 1.1. A *perfect matching* on V is a matching wtih n edges.

With this in mind, we ask; when does a bipartite graph have a perfect matching? To start, if a graph does not admit a perfect matching, then there exists a subset of L in which the number of neighbors is less than the number of elements in the set. Formally writing, if G has a perfect matching, then for all subsets $S \subseteq L$, $|N(S)| \geq |S|$ (where $N(S)$ represents the set of neighbors of S). Similarly, its contrapositive states that if there exists some $S \subseteq L$ such that $|N(S)| < |S|$, then there does not exist a perfect matching.

Theorem 1.2 (Hall's Theorem)**.** If G does not have a perfect matching, then there exists $S \subseteq L$ such that $|N(S)| \leq |S|$.

We start with an inductive proof on n. Start with a graph G such that for all $S \subseteq L$, $|N(S)| \geq |S|$; we want to find a perfect matching for G. Proceed with casework;

[1] additional details on example choices of α, β omitted because i'm garbage at using tikz

- In the first case (in which there is slack), suppose that for all nonempty, non-whole subsets $S \subseteq L$, $|N(S)| \geq |S|$. Take any edge $e = (x, y) \in E$, and delete it to get $G' = (L \setminus \{x\}, R \setminus \{y\}, E')$, where $E' = E \setminus \{e\}$. Then G' satisfies the inductive hypothesis, without slack.
- In the second case (in which there is no slack), there exists $S \subseteq L$ such that $S \neq \emptyset, L$ such that $|N(S)| = |S|$. Produce graph $G' = (S, N(S), E \cap (S \times N(S)))$. G' satisfies the inductive hypothesis, since its neighborhoods are the same as in G. For $T \subseteq S$, $N_{G'}(T) = N_G(T)$, so G' indeed has a perfect matching M'.

  Now, produce another graph $G'' = (L \setminus S, R \setminus N(S), E \cap (L \setminus S) \times (R \setminus N(S)))$; we want to show that G'' satisfies Hall's condition. Take $T \subseteq L \setminus S$; we have that $|N_G(T)| \geq |T|$. Consider $T \cup S$; $N_G(T \cup S) = N_G(S) \sqcup N_{G''}(T)$ and $|N_G(S)| = |S|$, so $|N_{G''}(T)| \geq |T|$. Thus, we conclude that G'' satisfies Hall's conditoion, and so it has a perfect matching M''. Then we may take $M = M' \cup M''$ as our desired perfect matching for G. □

Here are a handful of trivial algorithms to determine perfect matching;

(a) If we check all subsets of E, then it would take $2^{O(n^2)}$ time.

(b) All bijections between L, R, and check if the subsets of E work; this would take $O(n!) \leq n^n = 2^{O(n \log n)}$.

(c) Hall's condition takes $O(n^2 \cdot 2^n)$ time.[2]

We now present an algebraic algorithm for checking if a bipartite graph has a perect matching. Consider the $n \times n$ adjacency matrix A_G between L and R, where an entry is 1 if (x, y) is an edge (with $x \in L, y \in R$), and 0 otherwise. Now, replace each 1 in A_G with a random value in $[0, 1]$, and call the new matrix B_G. Compute $\det B_G$. If $\det B_G = 0$, then there is no perfect matching; otherwise, there is a perfect matching with probability 1.

Consider the variable adjacency matrix $M_G((x_e)_{e \in E})$, where $P(\vec{x}) = \det M_G(\vec{x})$, with $\vec{x} \in [0, 1]^E$. Compute $P(\vec{x})$. For example, if

$$M_G = \begin{pmatrix} x_1 & 0 \\ x_2 & 0 \end{pmatrix},$$

then $P(\vec{x}) = 0$. However, if

$$M_G = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix},$$

then $P(\vec{x}) = \det M_G = x_1 x_4 - x_2 x_3$. It is extremely unlikely that $P(\vec{x}) = 0$, and so we have our algorithm as desired.

Lemma 1.3. G has a perfect matching if and only if $p(\vec{x}) \neq 0$.

Lemma 1.4. If $Q(x_1, \ldots, x_m)$ is a nonzero polynomial, then

$$\Pr_{x \in [0,1]^m}[Q(x) = 0] = 0.$$

Lemma 1.5 (Schwartz-Zippel)**.** Let $S \subseteq \mathbb{F}$. If $Q(x_1, \ldots, x_m) \in \mathbb{F}[x_1, \ldots, x_m]$ is nonzero of degree $\leq d$, then

$$\Pr_{x \in S^m}[Q(x) = 0] \leq \frac{d}{|S|}.$$

[2] not sure what this means...

We will now prove this. To start,

$$P(\vec{x}) = \det M_Q(\vec{x}) = \sum_{\pi: L \to R} (-1)^{\operatorname{sgn}(\pi)} \prod_{u \in L} M_{(u,\pi(u))},$$

which is an equivalent expression to

$$\sum_{\substack{\text{perf. matchings} \\ \pi: L \to R}} \pm \prod_{u \in L} X_{(u,\pi(u))}.$$

The *permanent* here is essentially the number of perfect matchings. In general, determinants are easy to compute, but permanents are hard.

We now prove the Schwartz-Zippel lemma. Let $Q(x_1, \ldots, x_m)$ be nonzero with degree $\leq d$. We claim that the number of $a = (a_1, \ldots, a_n) \in S^n$ such that $Q(a) = 0$ is less than or equal to $d\,|S|^{n-1}$. Proceed by casework;

- For $m = 1$, by the fundamental theorem of algebra, an nonzero univariate polynomial of degree d has at most d roots.
- We now induct on m. Write

  $$Q(x_1, \ldots, x_m) = x_m^t Q_t(x_1, \ldots, x_{m-1}) + \cdots + Q_0(x_1, \ldots, x_{m-1})$$

  as a polynomial in x_m. Note that $\deg Q_i \leq d - i$, and that $Q_t \neq 0$. Let $B = \{(a_1, \ldots, a_{m-1}) \in S^{n-1} \mid Q_t(a_1, \ldots, a_{m-1}) = 0\}$. Then by the induction hypothesis, we have

  $$\Pr_{(a_1,\ldots,a_{n-1}) \in S^{n-1}}[(a_1, \ldots, a_{m-1}) \in B] \leq \frac{\deg Q_i}{|S|} \leq \frac{d-t}{|S|}.$$

  If $(a_1, \ldots, a_{m-1}) \notin B$, then

  $$\Pr_{a_m \in S}[Q(a_1, \ldots, a_m) = 0] \leq \frac{t}{|S|}.$$

  I don't entirely understand where this is going because it's notation hell, but I know the proof I guess. Read wikipedia link :p hehe.

Definition 1.6 (Doubly-Stochastic Matrix)**.** A doubly stochastic matrix is $M \in \mathbb{R}^{n \times n}$ such that $M_{ij} \geq 0$ for all i, j, and for all i, $\sum_j M_{ij} = 1$, and for all j, $\sum_i M_{ij} = 1$; i.e., the rows and columns sum to 1.

Every doubly stochastic matrix is a convex combination of permutation matrices. (Birkhoff's Theorem, here, and Theorem 5.5 in textbook)

Leaving off notes for today because I need to go find where MAT267 is.

§7 Day 7: More Probabilistic Methods (Feb. 26, 2025)

Today, we will discuss more probabilistic methods. We start with an example problem. Let us pick 10 numbers from $\{1, \dots, 100\}$. What is the probability that there exist distinct subsets A, B such that the sum of the elements in A is equal to the sum of the elements in B?

$$17, 38, 9, 29, 95, 66, 31, 12, 91, 13 \qquad \text{(Example Set)}$$

Let us consider this in a pigeonhole fashion; for each subset S (which we will denote as pigeons), we shall send them to their respective sums of elements (which we will denote as pigeonholes). To start, there are a total of 2^{10} pigeons (since each of the ten numbers may either be picked, or not picked, in forming a subset), and there are at most 1000 pigeons. Thus, there always exists such subsets A, B by the pigeonhole principle.

Theorem 7.1. Pick n numbers in $\{1, 2, \dots, F(n)\}$. Then there exist two subsets that have the same sum of elements.

We note that $F(n) = \frac{2^n}{n}$ works in this theorem. In particular, the sums of the numbers we picked lie in the set $\{n, \dots, nf(n)\}$ (and so there are $nf(n) - n + 1$ pigeonholes). If $f(n) < \frac{2^n}{n} - n$, then there always exist some hole with two pigeons, i.e., such two subsets exist.

Conjecture 7.2 (Erdos Conjecture)**.** There exists $f(n) = \Omega(2^n)$ that makes the theorem above true.

We seek to prove something simpler for now,

Theorem 7.3. We may take $f(n) = \Omega(\frac{2^n}{\sqrt{n}})$ for the theorem.

Let $M = \Omega(\frac{2^n}{\sqrt{n}})$, whose value is to be determined. We have $a_1, \dots, a_n \in \{1, \dots, M\}$, and we want to show that there exist two subsets of $\{a_1, \dots, a_n\}$ that have the same sum.

To do this, we give a random process that we will be working on. Let $X_1, \dots, X_n$ be independent random variables distributed $B(0.5)$, i.e. $X_1 = 0$ or 1 with equal probabilities. Let us consider the random set $S = \{a_i \mid X_i = 1\}$, and let Z be equal to the sum of the elements in S. Let us estimate $\mathbb{E}[Z]$ and $\mathrm{Var}(Z)$ to conclude there is a small interval I with $P[Z \in I] \geq 0.9$.[3] Directly write as follows,

$$\mathbb{E}[Z] = \mathbb{E}\left[\sum_{i=1}^{n} a_i X_i\right] = \sum_{i=1}^{n} \mathbb{E}[a_i X_i] = \frac{1}{2}\sum_{i=1}^{n} a_i.$$

For variance, let us write

$$\begin{aligned}
\mathrm{Var}(Z) = \mathbb{E}\left[\left(Z - \frac{1}{2}\sum_{i=1}^{n} a_i\right)^2\right] &= \mathbb{E}\left[\sum_{i=1}^{n}\left(a_i X_i - \frac{a_i}{2}\right)^2\right] \\
&= \mathbb{E}\left[\sum_{i,j=1}^{n} a_i\left(x_i - \frac{1}{2}\right) a_j\left(x_j - \frac{1}{2}\right)\right] \\
&= \sum_{i,j=1}^{n} a_i a_j \mathbb{E}\left[\left(X_i - \frac{1}{2}\right)\left(X_j - \frac{1}{2}\right)\right] \\
&= \sum_{i=1}^{n} a_i^2 \mathbb{E}\left[\left(X_i - \frac{1}{2}\right)^2\right] = \frac{1}{4}\sum_{i=1}^{n} a_i^2.
\end{aligned}$$

[3] 0.9 just happens to be good enough; we may refine this number more, but for the purposes of this proof, we choose a nice constant

Applying Chebyshev's inequality, as given below,

$$P(|Z-\mu|>t)\leq\frac{\mathrm{Var}(Z)}{t^2},$$

we obtain that the RHS in our situation is $\frac{1}{4t^2}\sum_{i=1}^n a_i^2$. Setting $t=10\sqrt{\frac{1}{4}\sum_{i=1}^n a_i^2}$, we have that $P(|Z-\mu|\geq t)\leq 0.1$, and so $P(Z\in[\mu-t,\mu+t])\geq 0.9$. In the acse that $0.9\cdot 2^n>2t$, by the pigeonhole principle, we have that there exists two subsets with the same sum of elements. Thus, we simply want

$$0.9\cdot 2^n>2\cdot 10\cdot\frac{1}{2}\cdot\sqrt{\sum_{i=1}^n a_i^2}=10\sqrt{\sum_{i=1}^n a_i^2}$$

In particular, we know that $10\sqrt{\sum_{i=1}^n a_i^2}\leq 10\sqrt{M^2n}=10\sqrt{n}M$. Thus, if

$$M<\frac{0.9\cdot 2^n}{10\sqrt{n}},$$

then our above desired inequality is satisfied. Now, we wish to find t such that there is a "collision", i.e. the event that there exists two distinct subsets that have the same sum. This occurs when we have

$$t<\frac{2^n}{2}\left(1-\frac{1}{k^2}\right);$$

If $\frac{k}{2}M\sqrt{n}<\frac{2^n}{2}(1-\frac{1}{k^2})$, then we have found a collision; thus, we just want

$$M<\frac{2^n}{\sqrt{n}}\left(\frac{1}{2}\left(1-\frac{1}{k^2}\right)\cdot\frac{2}{k}\right)=\frac{2^n}{\sqrt{n}k}\left(1-\frac{1}{k^2}\right).$$

We now introduce Sperner's lemma; to start, here is the prerequisite knowledge. Let S be a set, and let $\mathcal{P}(S)$ be its power set; then $\subseteq$ induces a partial ordering on $\mathcal{P}(S)$, where

- $a\subseteq a$ for all $a\in S$;
- $a\subseteq b$ and $b\subseteq a$ implies $a=b$;
- $a\subseteq b$ and $b\subseteq c$ implies $a\subseteq c$.

An *antichain* is a subset $F\subseteq\mathcal{P}(S)$ such that, for all $A,B\in F$, $A\subsetneq B$ and $B\subsetneq A$, i.e., a collection of *incomparable* subsets of S. To start, we may observe that $\binom{S}{m}$ is an antichain (i.e., the collection of all m-element subsets of S), and

$$\left|\binom{S}{m}\right|=\binom{n}{m}$$

is largest when $m=\lfloor n/2\rfloor$.

Lemma 7.4 (Sperner's Lemma)**.** Any antichain in $\mathcal{P}(S)$ has at most $\binom{n}{\lfloor n/2\rfloor}$ sets.

Let $a_1,\ldots,a_m$ be the elements of the antichain, and let π be a uniformly random permutation of $S=\{1,\ldots,n\}$. Define the event E_i to be that the first $|A_i|$ elements of this sequence equals A_i. For example, let $S=\{1,2,3,4\}$. Then if $A_1=\{1,2\},A_2=\{2,3,4\},A_3=\{1,4\}$, then

$$\begin{aligned}E_1&=\text{"}\{\pi(1),\pi(2)\}=\{1,2\}\text{"};\\E_2&=\text{"}\{\pi(1),\pi(2),\pi(3)\}=\{2,3,4\}\text{"};\\E_3&=\text{"}\{\pi(1),\pi(2)\}=\{1,4\}\text{"}.\end{aligned}$$

In particular,

$$P(E_1) = \frac{1}{\binom{4}{2}}, \quad P(E_2) = \frac{1}{\binom{4}{3}}, \quad P(E_3) = \frac{1}{\binom{4}{2}}.$$

Claim 7.5. The events E_i are disjoint.

Let E_i, E_j be distinct events, and suppose they both happen; then A_i, A_j are both prefixes of $\pi(1), \pi(2), \dots, \pi(n)$; but then $\{\pi(1), \dots, \pi(|a_i|)\}$ and $\{\pi(1), \dots, \pi(|a_j|)\}$ are both comparable, which contradicts our assumption.

Thus, we must have that

$$\sum_i P(E_i) \le 1 \implies \sum_{i=1}^{m} \frac{1}{\binom{n}{|A_i|}} \le 1.$$

In particular,

$$1 \ge \sum_{i=1}^{m} \frac{1}{\binom{n}{|A_i|}} \ge \frac{M}{\binom{n}{\lfloor n/2 \rfloor}} \implies m \le \binom{n}{\lfloor n/2 \rfloor}.$$

We now move onto the Littlewood Offord Problem. Let $a_1, \dots, a_n \in \mathbb{R}$ be nonzero, and pick i.i.d. random Rademacher variables $\varepsilon_1, \dots, \varepsilon_n \in \{\pm 1\}$. Consider $P(\sum_{i=1}^n \varepsilon_i a_i = 0)$. How high can this probability be? Littlewood and Offord showed that the probability is always less than or equal to $O(\frac{1}{n^{0.4}})$ using very difficult methods. Erdos showed that the probability is less than or equal to

$$\frac{\binom{n}{\lfloor n/2 \rfloor}}{2^n} = \Theta\left(\frac{1}{\sqrt{n}}\right).$$

This bound is tight, since if n is even and $a_1, \dots, a_n = 1$, then

$$P\left(\sum_{i=1}^{n} \varepsilon_i a_i = 0\right) = \frac{\binom{n}{n/2}}{2^n}.$$

We now prove the Erdos bound. Assume, since we are already using Rademacher variables, that each a_i is positive. For each $\vec{\varepsilon} \in \{\pm 1\}^n$, define $A(\vec{\varepsilon}) \subseteq [n]$, where $A(\vec{\varepsilon}) = \{i \in [n] \mid \varepsilon_i = 1\}$, i.e., the collection of indices such that $\varepsilon_i = 1$. Then we have that

$$\sum_{i=1}^{n} \varepsilon_i a_i = 2\left(\sum_{i \in A(\vec{\varepsilon})} a_i\right) - \left(\sum_{i \in [n]} a_i\right).$$

If $\sum_{i=1}^n \varepsilon_i a_i = 0$ and $\sum_{i=1}^n \varepsilon_i' a_i = 0$ (where ε' is another vector of Rademacher variables), then

$$\sum_{i \in A(\vec{\varepsilon})} a_i = \sum_{i \in A(\vec{\varepsilon'})} a_i.$$

In particular, this means that $A(\vec{\varepsilon})$ and $A(\vec{\varepsilon'})$ are incomparable. Now, let us consider the family

$$\mathcal{F} = \{A(\vec{\varepsilon}) \mid \sum_{i=1}^{n} \varepsilon_i a_i = 0; \vec{\varepsilon} \in \{\pm 1\}^n\};$$

from earlier, we see that $\mathcal{F}$ is indeed an antichain. By Sperner's lemma, we now have that $|\mathcal{F}| \le \binom{n}{n/2}$, and so

$$|\{\vec{\varepsilon} \in \{\pm 1\}^n \mid \langle \vec{\varepsilon}, a \rangle = 0\}| \le \binom{n}{\lfloor n/2 \rfloor}.$$

Now, let us consider unit vectors $v_1, \dots, v_n \in \mathbb{R}^m$.

Claim 7.6. There is a signing $\varepsilon_1, \dots, \varepsilon_n \in \{\pm 1\}$ such that

$$\left\| \sum_{i=1}^n \varepsilon_i v_i \right\|_2 \le \sqrt{n}.$$

Similarly, there exists a signing such that

$$\left\| \sum_{i=1}^n \varepsilon_i v_i \right\|_2 \ge \sqrt{n}.$$

Note that we have

$$\mathbb{E}\left[\left\| \sum_{i=1}^n \varepsilon_i v_i \right\|_2^2 \right] = n.$$

Choose $(\varepsilon_1, \dots, \varepsilon_n) \in \{\pm 1\}^n$ uniformly, where the ε_i are i.i.d. Rademacher. Consider $\sum_{i=1}^n \varepsilon_i v_i$; while we cannot study

$$\mathbb{E}\left[\left\| \sum_{i=1}^n \varepsilon_i v_i \right\|_2 \right]$$

as easily, we have that

$$\begin{aligned} \mathbb{E}\left[\left\| \sum_{i=1}^n \varepsilon_i v_i \right\|_2^2 \right] &= \mathbb{E}\left[\left\langle \sum_i \varepsilon_i v_i, \sum_j \varepsilon_j v_j \right\rangle \right] \\ &= \mathbb{E}\left[\sum_{i,j} \varepsilon_i \varepsilon_j \langle v_i, v_j \rangle \right] \\ &= \sum_{i,j} \langle v_i, v_j \rangle \, \mathbb{E}[\varepsilon_i \varepsilon_j] = \sum_i \|v_i\|^2 = n. \end{aligned}$$

The average norm squared as ε varies over all choices. Therefore, there is some signing such that the norm squared is at least n, some signing that it is at most n, which implies our claim from earlier.

Next class, we will study Ramsay theory.

§10 Day 10: Linear Algebraic Methods (Mar. 19, 2025)

We start with an example problem.

Claim 10.1. Let a 1-distance set be denoted as an *equilateral set*; specifically, such a set has the property that, for $x_1, \dots, x_n \in S \subset \mathbb{R}^d$, we have $\|x_i - x_j\|_2 = 1$ for any two distinct i, j. We claim that $n := |S| = d+1$ is the largest possible size of such equilateral sets.

Visually, we can picture this problem by considering the intersections between unit balls in $\mathbb{R}^d$. If $d = 2$, then the optimal n is 3. If $d = 3$, we have $n = 4$. In general, for any given d, we have that $n = d + 1$. Let us try to prove this by inducting on d.

For any d points, there is a $(d-1)$-dimensional plane H containing them. Specifically, let these points be called $z_1, \dots, z_d$. We want an equation

$$\left\langle a, \vec{X} \right\rangle = b$$

defining H such that $\langle a, z_i \rangle = b$ for all $i = 1, \dots, d$. In particular, we want $\vec{a}, b$ such that

$$b = \langle \vec{a}, \vec{z} \rangle ,$$

where $\vec{z} = (z_1, \dots, z_d)$. By observing the rank, there must exist such nonzero $\vec{a}$ and b. Let H be a $(d-1)$-dimensional hyperplane containing $z_1, \dots, z_d$. We know, by definition, that no other x_i is in H. Suppose $y, z \in \mathbb{R}^t \setminus H$ such that $\|y - x_i\| = 1$, $\|z - x_i\| = 1$, and $\|y - z\| = 1$ for all $i \le d$. We want to use this to obtain a contradiction. By translating, assuime that the point is the origin. If $n \ge d + 1$, then we get $x_1, \dots, x_{d+1} \in \mathbb{R}^d$ such that $\|x_i\| = 1$ and $\|x_i - x_j\| = 1$.

i don't particularly like this direction of proof... just take isometry to regular simplices.

Claim 10.2. Let a 2-distance set be a collection of points $x_1, \dots, x_n \in \mathbb{R}^d$ with $A, B \in \mathbb{R}$ such that, for all $i \ne j$, we have $\|x_i - x_j\|$ is equal to A or B.

§12 Day 12: Fourier Analysis on Finite Fields (Apr. 2, 2025)

For each $a \in \mathbb{F}_2^n$, let $\psi_a : \mathbb{F}_2^n \to \mathbb{C}$, where $\psi_a(x) = (-1)^{\langle a,x\rangle}$. Then we have the three following properties;

(i) The ψ_a are a basis for $\mathcal{C}^{(\mathbb{F}_2^n)} = \{f : \mathbb{F}_2^n \to \mathbb{C}\}$,

(ii) We have the following sum,

$$\sum_{x\in\mathbb{F}_2^n} \psi_a(x)\psi_b(x) = \begin{cases} 0 & a \neq b, \\ 2^n & a = b. \end{cases}$$

(iii) For any $f : \mathbb{F}_2^n \to \mathbb{C}$, we can write $f = \sum_{a\in\mathbb{F}_2^n} \hat{f}(a)\psi_a$, where $\hat{f}$ is given by

$$\hat{f}(a) = \frac{1}{2^n} \sum_{x\in\mathbb{F}_2^n} f(a)\psi_a(x).$$

Now, let $S \subseteq \mathbb{F}_2^n$, and consider the indicator $1_S : \mathbb{F}_2^n \to \mathbb{C}$, given by $1_S = \sum_a \hat{1}_S(a)\psi_a$. Consider the hypercube graph $V = \{0,1\}^n$, and E being the edge set, consisting of pairs of vertices that differ in 1 coordinate. Then for any subset $S \subseteq \{0,1\}^n$, we say that the edge neighborhood is the collection of edges between S and S^C. How small can the edge neighborhood of S be if $|S| = \alpha 2^n$? It is easy to see that, for a random set of density α, we can expect $n(1-\alpha)(\alpha 2^n)$ edges to go from S to S^C. This will be our trivial upper bound; we now check more details.

Consider the subcube of $\{0,1\}^n$ given by the collection of all vertices $x \in \{0,1\}^n$ such that their first k components are 0. Then we have that its size is $2^{n-k} = \alpha 2^n$, and its edge boundary is $k2^{n-k} = \log(\alpha^{-1})\alpha 2^n$, which is asymptotically smaller than our previous expected size.

The Hamming ball β_r is defined as the collection of vertices on $x \in \{0,1\}^n$ such that the number of 1s in x is less than or equal to r. Then the edge boundary has $\binom{n}{r}(n-r)$ elements, where

$$|\beta_r| = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{r}.$$

What shuold r be such that $\alpha 2^n = |\beta_r|$? Set $n = \frac{n}{2} - c_\alpha\sqrt{n}$. Then we have that the number of elements in the edge boundary is given by

$$(n-r)\binom{n}{r} \approx n\left(\frac{1}{2} + \frac{c_\alpha}{\sqrt{n}}\right)\Theta\left(\frac{2^n}{\sqrt{n}}\right) = \Theta(\sqrt{n}2^n),$$

with the last equality being given when $\alpha = \Theta(1)$.

We can also describe the edge boundary of S in terms of $\hat{1}_S$. In this manner, the number of elements in the edge boundary of S is given by

$$\sum_{x\in\mathbb{F}_2^n} 1_S(a)\left(\sum_{i=1}^{n}(1 - 1_S(x+e_i))\right).$$

We may directly evaluate this expression.

$$\begin{aligned}
&\sum_{x\in\mathbb{F}_2^n} 1_S(a)\left(\sum_{i=1}^{n}(1-1_S(x+e_i))\right)\\
&=\sum_{x\in\mathbb{F}_2^n}\sum_i 1_S(x)-\sum_{x\in\mathbb{F}_2^n}\sum_i 1_S(x)1_S(x+e_i)\\
&=\alpha n2^n-\sum_{x\in\mathbb{F}_2^n}\sum_{i\in[n]}\left(\sum_a \hat{1}_S(a)\psi_a(x)\right)\left(\sum_b \hat{1}_S(b)\psi_b(x+e_i)\right)\\
&=\alpha n2^n-\sum_{a,b}\hat{1}_S(a)\hat{1}_S(b)\left(\sum_x \psi_a(x)\psi_b(x)\left(\sum_i \psi_b(e_i\right)\right)\\
&=\alpha n2^n-\sum_{a,b}\hat{1}_S(a)\hat{1}_S(b)2^n 1_{a-b}\left(\sum_i \psi_b(e_i)\right)\\
&=\alpha n2^n-\sum_a \hat{1}_S(a)^2\cdot 2^n\cdot\sum_{i\in[n]}\psi_a(e_i)\\
&=\alpha n2^n-\sum_a \hat{1}_S(a)^2\cdot 2^n\cdot(n-2\mathrm{wt}(n))\\
&=\alpha n2^n-\left(\sum_a \hat{1}_S(a)^2\cdot 2^n\cdot n\right)+\sum_a \hat{1}_S(a)^2(n-2\mathrm{wt}(a))2^n\\
&=\sum_a \hat{1}_S(a)^2\left(2\mathrm{wt}(a)\right)2^n\\
&\le\sum_a \hat{1}_S(a)^2(2n)2^n<2n(\alpha 2^n).
\end{aligned}$$

We skip a few details from class, yadayada. Anyways. Let $S\subseteq\mathbb{F}_2^n$¿ Let $|S|=\alpha 2^n$. Let $\hat{1}_S(0)=\alpha$. Suppose $\left|\hat{1}_S(a)\right|\le\varepsilon\alpha$ for all $a\neq 0$. What is the size of $\{(x,y,z)\in S\mid z=x+y\}$?