Electronic Colloquium on Computational Complexity, Report No. 148 (2021)

EXPLICIT EXPONENTIAL LOWER BOUNDS FOR EXACT HYPERPLANE COVERS

Benjamin E. Diamond
Core Cryptography
Coinbase
benediamond@gmail.com

Amir Yehudayoff
Department of Mathematics
Technion – IIT
amir.yehudayoff@gmail.com

Abstract

We describe an explicit and simple subset of the discrete hypercube which cannot be exactly covered by fewer than exponentially many hyperplanes. The proof exploits a connection to communication complexity, and relies heavily on Razborov's lower bound for disjointness.

1 Introduction

The relationship between hyperplanes in Euclidean space and the discrete hypercube is fundamental and important. One basic problem entails understanding the number of hyperplanes which one must use to cover various subsets of the cube. A *hyperplane* is specified by a normal vector $(a_1, \ldots, a_n) \in \mathbb{R}^n$ and an offset $w \in \mathbb{R}$, defined specifically as the set $H = \{x \in \mathbb{R}^n \mid \sum_{i=1}^n a_i \cdot x_i = w\}$. A collection of hyperplanes $H_1, H_2, \ldots, H_N$ *exactly covers* a set $S \subseteq \{0,1\}^n$ if $\bigcup_{i=1}^N H_i \cap \{0,1\}^n = S$. The *exact cover number* $\mathrm{ec}(S)$ of a set S is the minimum cardinality N attained across all hyperplane configurations exactly covering S.

The exact cover number $\mathrm{ec}(\{0,1\}^n)$ of the full cube is 2. Seminal work of Alon and Füredi [AF93] shows that removing a single point makes exact covering much harder; the exact cover number of $\{0,1\}^n \setminus \{(0,\ldots,0)\}$ is n. The study of exact covers of arbitrary sets appears in recent work of Aaronson, Groenland, Grzesik, Johnston, and Kielak [AGG$^+$21]. That work focuses on worst-case cardinalities of the form $\mathrm{ec}(n) := \max_{S \subseteq \{0,1\}^n} \mathrm{ec}(S)$; it proves that $\mathrm{ec}(n)$ is between $\frac{2^n}{n^2}$ and $2^{n-\lfloor \log n \rfloor} < 2 \cdot \frac{2^n}{n}$. The work's lower bound on $\mathrm{ec}(n)$ is not explicit, as it relies on a generic counting argument.

In this work, we analyze $\mathrm{ec}(S)$ for concrete subsets $S \subseteq \{0,1\}^n$. Beyond this problem's intrinsic appeal, an additional strong source of motivation stems from forthcoming work by the first-listed author [Dia21], which links exact hyperplane covers to secure two-party computation. This work shows that exact covers yield protocols for secure computation by two malicious parties. The work's protocols, moreover, are efficient when the exact cover number is small. It is of interest, therefore, to determine which set families are and are not efficiently coverable.

Our main result exhibits a concrete set $D_n \subseteq \{0,1\}^n$ for which $\mathrm{ec}(D_n)$ grows exponentially in n. The definition of D_n is extremely simple; D_n consists of those pairs $(x,y) \in \{0,1\}^{n/2} \times \{0,1\}^{n/2} \cong \{0,1\}^n$ for which the bitwise AND of x and y is identically zero (for simplicity, we assume that n is even). In other words, D_n consists exactly of those pairs (x,y) for which x and y, interpreted as *sets*, are disjoint.[1]

Theorem. $\mathrm{ec}(D_n) \geq 2^{\Omega(n)}$.

We briefly discuss a further interpretation of the theorem, developed in [Dia21]. Exact cover numbers can be understood as furnishing a sort of complexity measure on boolean functions. To each boolean function $f : \{0,1\}^n \to \{0,1\}$, we may associate the complexity measure $\mathrm{ec}(f) := \max\left\{\mathrm{ec}(f^{-1}(0)), \mathrm{ec}(f^{-1}(1))\right\}$, for example. The relationship between this latter complexity measure and other, more standard, complexity measures is not yet fully understood.

[1] We focus throughout on hyperplanes H defined over the reals. Our results, however, carry through to *any* field, and even to "hyperplanes" defined over $\mathbb{Z}$.

ISSN 1433-8092

For example, if f is symmetric[2] (as *parity* and *majority* are), then $\mathrm{ec}(f)$ is at most $n+1$. The theorem, on the other hand, shows that the exact cover complexity of the boolean function $(x,y) \mapsto \bigvee_{i=1}^{n/2} x_i \wedge y_i$ is exponential in n. This demonstrates a strong separation between exact cover complexity and monotone depth-two circuit complexity.

We prove our lower bound on the exact cover number of D_n by upper-bounding the sizes of certain sets of the form $H \cap D_n$, where $H \subseteq \mathbb{R}^n$ is a hyperplane. No strong such upper bound, of course, can possibly hold for all hyperplanes. We say that a hyperplane H is *contained* in a set $S \subseteq \{0,1\}^n$ if $H \cap \{0,1\}^n \subseteq S$. If H is contained in S, then, trivially, $|H \cap \{0,1\}^n| \leq |S|$ holds. The following lemma establishes an exponential improvement in the *particular* case of D_n:

Lemma. *If a hyperplane $H \subseteq \mathbb{R}^n$ is contained in D_n then $|H \cap \{0,1\}^n| \leq 2^{-\Omega(n)} \cdot |D_n|$.*

The lemma may be interpreted as a strong—though restricted—anti-concentration result. Classical anti-concentration results concern expressions of the form $\max_{w \in \mathbb{R}} \Pr\left[\sum_{i=1}^n a_i \cdot X_i = w\right]$, where X is uniformly distributed in $\{0,1\}^n$. The *Littlewood–Offord problem* entails establishing anti-concentration when all of the coordinates of $(a_1, \ldots, a_n)$ are assumed to be nonzero [LO43]; the problem's original motivation arose from the study of roots of random polynomials. Littlewood and Offord proved the preliminary upper bound of $O\left(\frac{\log n}{\sqrt{n}}\right)$. In a celebrated and sharp result, Erdős [Erd45] solved the Littlewood–Offord problem, proving the upper bound $2^{-n} \cdot \binom{n}{\lfloor n/2 \rfloor} \leq O\left(\frac{1}{\sqrt{n}}\right)$ using Sperner's theorem on the sizes of antichains. Kleitman [Kle65], Frankl and Füredi [FF88], Griggs [Gri93], and others subsequently generalized the problem.

The lemma says that for each normal $a \in \mathbb{R}^n$, we have $\max_w \Pr\left[\sum_{i=1}^n a_i \cdot X_i = w\right] \leq 2^{-\Omega(n)} \cdot \Pr[X \in D_n]$, where the maximum is taken *not* over all constants $w \in \mathbb{R}$, but rather over only those for which the hyperplane $\{x \in \mathbb{R}^n \mid \sum_{i=1}^n a_i \cdot x_i = w\}$ is contained in D_n. The lemma holds for all a, and guarantees *exponentially* strong anti-concentration; on the other hand, the bound holds only for certain w. The fact that the bound holds only for some among the values w makes it difficult to use known techniques to prove anti-concentration (like extremal combinatorics, or Fourier analysis).

Our main high-level contribution is a bridge between this sort of restricted anti-concentration and two-party communication complexity (see the textbook [RY20] and references within). Our proof follows the ideas of Razborov's [Raz92] famous lower bound for the distributional two-party communication complexity of disjointness. This bridge is built by means of a certain decomposition on hyperplane intersections. For each hyperplane $H = \left\{(x,y) \in \{0,1\}^{n/2} \times \{0,1\}^{n/2} \,\middle|\, \sum_{i=1}^{n/2} a_i \cdot x_i + \sum_{i=1}^{n/2} b_i \cdot y_i = w\right\}$, we have:

$$H \cap D_n = \bigcup_{k \in \mathbb{R}} (A_k \times B_k) \cap D_n, \tag{1}$$

where $A_k := \left\{x \in \{0,1\}^{n/2} \,\middle|\, \sum_{i=1}^{n/2} a_i \cdot x_i = k\right\}$ and $B_k := \left\{y \in \{0,1\}^{n/2} \,\middle|\, \sum_{i=1}^{n/2} b_i \cdot y_i = w - k\right\}$. In the language of communication complexity, for each k, the set $(A_k \times B_k) \cap D_n$ is a *rectangle* (i.e., a product set in $\{0,1\}^{n/2} \times \{0,1\}^{n/2}$); the assumption $H \subseteq D_n$ implies that each rectangle $(A_k \times B_k) \cap D_n$ is *1-monochromatic*. In a nutshell, we see that if $\mathrm{ec}(D_n)$ were small, then D_n would resemble the on-set of a function whose communication complexity was small. The full picture is in fact subtler, as we explain below.

The crux of Razborov's lower bound asserts that, in the setting of disjointness, all 1-monochromatic rectangles are small. To assess their sizes, Razborov carefully constructs a certain probability measure on the cube, and proves that each 1-monochromatic rectangle has exponentially small mass—say, $2^{-\varepsilon \cdot n}$—under this measure. We must surmount a few barriers in order to apply Razborov's ideas in our context.

The first among these barriers concerns the possible number of values k in the union expression above. In communication complexity, the goal is to prove that the number of values k is large. The bound of $2^{-\varepsilon \cdot n}$ on the mass of each individual rectangle—together with a "union bound"—then implies that there must be at least $2^{\varepsilon \cdot n}$ rectangles. In our setting, the possible number of values k can be much larger than $2^{\varepsilon \cdot n}$, and even as large as $3^{n/2}$; this makes the union bound useless. The key observation which overcomes this barrier is that our rectangles have a very specific structure; indeed, the sets $\{A_k\}_{k \in \mathbb{R}}$ are themselves pairwise disjoint in $\{0,1\}^{n/2}$, and likewise for the sets $\{B_k\}_{k \in \mathbb{R}}$. This observation, together with a more careful analysis, allows us to overcome the first barrier.

[2] That is, invariant under arbitrary permutations of its inputs.

Remark. We exploit the structure of H as a hyperplane during our proof *only* in our use of this simple property of the sets $\{A_k\}_{k\in\mathbb{R}}$ and $\{B_k\}_{k\in\mathbb{R}}$.

A second barrier that we must overcome stems from the fact that the distribution on D_n we consider is uniform; Razborov's argument exploits a carefully constructed distribution. This difference introduces several technical difficulties. Roughly, we use *measure concentration* to reduce our problem to a setting closer to Razborov's; we then analyze a "perturbed" variant of his distribution.

We suspect that our bound is not sharp:

Conjecture. *If a hyperplane $H \subseteq \mathbb{R}^n$ is contained in D_n, then $|H \cap \{0,1\}^n| \leq 2^{n/2}$.*

Remark. This conjecture is sharp, in that there exist hyperplanes H in D_n which satisfy $H \cap \{0,1\}^n = 2^{n/2}$.

2 Proving the Lemma

We fix even n and a hyperplane $H = \left\{(x,y) \in \{0,1\}^{n/2} \times \{0,1\}^{n/2} \,\middle|\, \sum_{i=1}^{n/2} a_i \cdot x_i + \sum_{i=1}^{n/2} b_i \cdot y_i = w\right\} \subseteq \mathbb{R}^n$, which we moreover assume is contained in $D := D_n$. We write μ for the uniform distribution on $D \subseteq \{0,1\}^n$. We partition D along the sizes of its two constituent sets, in the following way (recall that we understand x and y as sets, and so $|x|$ and $|y|$ respectively denote the cardinalities of x and y). For integers ℓ_x and ℓ_y in $\{0, \dots, \frac{n}{2}\}$, we set:

$$D_{\ell_x,\ell_y} := \left\{(x,y) \in \{0,1\}^{n/2} \times \{0,1\}^{n/2} \,\middle|\, |x| = \ell_x \wedge |y| = \ell_y\right\}.$$

We first argue that all but an exponentially vanishing proportion of the mass of μ is concentrated within those D_{ℓ_x,ℓ_y} for which both ℓ_x and ℓ_y are *simultaneously* near $\frac{n}{6}$.

Claim 2.1. *For each constant $\delta > 0$, we have $\mu\left(\bigcup_{n\cdot(\frac{1}{6}-\delta)\leq \ell_x,\ell_y \leq n\cdot(\frac{1}{6}+\delta)} D_{\ell_x,\ell_y}\right) > 1 - 2^{-\Omega(n)}$.*

Proof. A pair (X,Y) distributed according to μ may be sampled using $\frac{n}{2}$ i.i.d. pairs $(X_1,Y_1),\dots,(X_{n/2},Y_{n/2})$, each uniform in $\{(0,0),(0,1),(1,0)\}$. The expected values of $\sum_{i=1}^{n/2} X_i$ and of $\sum_{i=1}^{n/2} Y_i$ are exactly $\frac{n}{6}$. The union bound, together with a standard application of Chernoff's bound, completes the proof. □

We write μ_{ℓ_x,ℓ_y} for the distribution μ conditioned on D_{ℓ_x,ℓ_y}. In light of Claim 2.1, it suffices to prove that $\mu_{\ell_x,\ell_y}(H) \leq 2^{-\Omega(n)}$ holds whenever ℓ_x and ℓ_y simultaneously reside in $\left[n\cdot(\frac{1}{6}-\delta), n\cdot(\frac{1}{6}+\delta)\right]$, for some appropriate fixed $\delta > 0$. Throughout the remainder of the proof, we fix $\delta := \frac{1}{300}$, as well as arbitrary integers ℓ_x and ℓ_y in $\left[\frac{49}{300}\cdot n, \frac{51}{300}\cdot n\right]$. To bound $\mu_{\ell_x,\ell_y}(H)$, we use the decomposition (1). For fixed $k \in \mathbb{R}$, we write:

$$A_k := \left\{x \in \{0,1\}^{n/2} \,\middle|\, \textstyle\sum_{i=1}^{n/2} a_i \cdot x_i = k\right\} \quad \text{and} \quad B_k = \left\{y \in \{0,1\}^{n/2} \,\middle|\, \textstyle\sum_{i=1}^{n/2} b_i \cdot y_i = w - k\right\}.$$

A key step in our proof involves sampling from μ_{ℓ_x,ℓ_y} in a more informative way.

Remark. We denote random variables by capital letters, and and by lowercase letters the values they attain. In what follows, we impose the further assumption whereby $\frac{n}{2}$ is odd,[3] so that $m := \frac{n-2}{4}$ is an integer.

We write $T := (Z_x, Z_y, \{I\})$ for a uniformly random partition of $\{1,\dots,\frac{n}{2}\}$ into subsets sized exactly m, m, and 1, respectively. We write X for a uniformly random subset of $Z_x \cup \{I\}$ of cardinality exactly ℓ_x and Y for a uniformly random subset of $Z_y \cup \{I\}$ of cardinality exactly ℓ_y (X and Y are chosen independently). We moreover write X_0 and Y_0 for X and Y conditioned on $I \notin X$ and $I \notin Y$, respectively. Finally, we write X_1 and Y_1 for X and Y conditioned on $I \in X$ and $I \in Y$, respectively.

[3] This restriction is not necessary, but simplifies notation below.

2.1 Preliminary claims

Claim 2.2. *For each $k \in \mathbb{R}$, as the partition $t = (z_x, z_y, \{i\})$ varies, the numbers* $\Pr[X \in A_k \mid T = t]$ *and* $\Pr[Y_0 \in B_k \mid T = t]$ *depend only on z_y and the numbers* $\Pr[Y \in B_k \mid T = t]$ *and* $\Pr[X_0 \in A_k \mid T = t]$ *depend only on z_x.*

Claim 2.3. *For each fixed scalar $k \in \mathbb{R}$ and partition $t = (z_x, z_y, \{i\})$, we have*

$$\Pr[X_0 \in A_k \mid T = t] \leq \tfrac{25}{8} \cdot \Pr[X \in A_k \mid T = t]$$

and

$$\Pr[Y_0 \in B_k \mid T = t] \leq \tfrac{25}{8} \cdot \Pr[Y \in B_k \mid T = t].$$

Proof. We prove only the first conclusion; the second is similar. By the definitions of the distributions X and X_0, we have the bound $\Pr[X \in A_k \mid T = t] \geq \Pr[i \notin X \mid T = t] \cdot \Pr[X_0 \in A_k \mid T = t]$. The proportion of ℓ_x-element subsets of $z_x \cup \{i\}$ which don't contain i is $\Pr[i \notin X] = \frac{\binom{m}{\ell_x}}{\binom{m+1}{\ell_x}} = \frac{m+1-\ell_x}{m+1} \geq 1 - \frac{n}{n+2} \cdot \frac{204}{300} \geq \frac{8}{25}$. □

Definition 2.4. For each $k \in \mathbb{R}$, we define sets of "good" partitions in the following way:

$$G_x^k := \left\{ t = (z_x, z_y, \{i\}) \,\middle|\, \Pr[X_1 \in A_k \mid T = t] \geq \tfrac{1}{70} \cdot \Pr[X_0 \in A_k \mid T = t] - 2^{-\varepsilon \cdot n} \right\}$$

and

$$G_y^k := \left\{ t = (z_x, z_y, \{i\}) \,\middle|\, \Pr[Y_1 \in B_k \mid T = t] \geq \tfrac{1}{70} \cdot \Pr[Y_0 \in B_k \mid T = t] - 2^{-\varepsilon \cdot n} \right\},$$

where $\varepsilon := \frac{1}{600}$.

Claim 2.5. *For each fixed scalar $k \in \mathbb{R}$, and arbitrary fixed subsets z_x and z_y of $\{1, \ldots, \frac{n}{2}\}$, we have:*

$$\Pr\left[T \notin G_x^k \mid Z_y = z_y\right] < \tfrac{1}{7}$$

and

$$\Pr\left[T \notin G_y^k \mid Z_x = z_x\right] < \tfrac{1}{7}.$$

Proof. We prove only the first inequality, as the second is similar. We first handle the case in which $\Pr[X \in A_k \mid Z_y = z_y] < 2^{-\varepsilon \cdot n}$. In light of Claim 2.2, we note that $\Pr[X \in A_k \mid Z_y = z_y] = \Pr[X \in A_k \mid T = t]$ holds for each *particular* partition t drawn from the distribution $(Z_x, z_y, \{I\})$. Using Claim 2.3, we see that if any particular such t moreover satisfied $t \notin G_x^k$, then we would have:

$$\Pr[X_1 \in A_k \mid T = t] < \tfrac{1}{70} \cdot \Pr[X_0 \in A_k \mid T = t] - 2^{-\varepsilon \cdot n} \leq \tfrac{1}{20} \cdot \Pr[X \in A_k \mid T = t] - 2^{-\varepsilon \cdot n} < 0,$$

a contradiction, so that $\Pr\left[T \notin G_x^k \mid Z_y = z_y\right] = 0$, and the claim is proved.

We thus assume that $\Pr[X \in A_k \mid Z_y = z_y] \geq 2^{-\varepsilon \cdot n}$. We write $\overline{z_y}$ for the complement of z_y in $\{1, \ldots, \frac{n}{2}\}$, and abbreviate $\widehat{A}_k := A_k \cap \binom{\overline{z_y}}{\ell_x}$ for the set of ℓ_x-element subsets of $\overline{z_y}$ which *also* reside in A_k. We note that:

$$\Pr[X \in A_k \mid Z_y = z_y] = \frac{\left|\widehat{A}_k\right|}{\binom{m+1}{\ell_x}}.$$

We moreover record the lower bound

$$\log_2 \binom{m+1}{\ell_x} \geq \log_2 \binom{m+1}{\left\lfloor \frac{204}{300} \cdot (m+1) \right\rfloor} \geq (0.9 - o(1)) \cdot (m+1);$$

the last inequality is a standard consequence of Stirling's approximation, together with the binary entropy inequality $H\left(\frac{204}{300}\right) > 0.9$.

We write $\widehat{X}$ for a uniformly random element of $\widehat{A}_k$. For each fixed partition $t = (z_x, z_y, \{i\})$, we have:

$$\Pr[X \in A_k \mid T = t] \cdot \Pr\left[i \in \widehat{X}\right] = \Pr[X_1 \in A_k \mid T = t] \cdot \Pr[i \in X \mid T = t] = \Pr[X_1 \in A_k \mid T = t] \cdot \frac{\binom{m}{\ell_x - 1}}{\binom{m+1}{\ell_x}},$$

which in turn equals

$$\Pr\left[X_1 \in A_k \mid T = t\right] \cdot \frac{\ell_x}{m+1} \leq \Pr\left[X_1 \in A_k \mid T = t\right] \cdot \tfrac{17}{25}.$$

By the above inequality and Claim 2.3, we see that if moreover $t \notin G_x^k$ holds, then we have:

$$\Pr\left[X \in A_k \mid T = t\right] \cdot \Pr[i \in \widehat{X}] < \tfrac{1}{100} \cdot \Pr\left[X_0 \in A_k \mid T = t\right] \leq \tfrac{1}{30} \cdot \Pr\left[X \in A_k \mid T = t\right],$$

so that $\Pr\left[i \in \widehat{X}\right] < \frac{1}{30}$. Equivalently, if the partition $t = (z_x, z_y, \{i\})$ is not "good", then the component of the joint distribution $\widehat{X}$ corresponding to the element $i \in \overline{z_y}$ has success probability less than $\frac{1}{30}$.

We write $\widehat{X}_j$ for the indicator function of the event $i_j \in \widehat{X}$, where $\{i_1, \ldots, i_{m+1}\}$ are the elements of $\overline{z_y}$, so that $\widehat{X} = (\widehat{X}_1, \ldots, \widehat{X}_{m+1})$. We observe that if the claim were false—and, in particular, $\Pr[i \in \widehat{X}] \leq \dfrac{1}{30}$ held for at least $\frac{1}{7}$ among the $m+1$ elements $i \in \overline{z_y}$—then the binary entropy of $\widehat{X}$ would satisfy:

$$\begin{aligned}
(0.9 - o(1) - 5\varepsilon) \cdot (m+1) &\leq H(\widehat{X}) && \text{(by } \Pr\left[X \in A_k | T = t\right] \geq 2^{-\varepsilon \cdot n} \text{ and } |\widehat{A}_k|\text{)} \\
&\leq \sum_{j=1}^{m+1} H(\widehat{X}_j) && \text{(by the sub-additivity of entropy)} \\
&< \left(\tfrac{6}{7} + \tfrac{1}{7} \cdot H(\tfrac{1}{30})\right) \cdot (m+1) && \text{(by the assumption that the claim is false)} \\
&\leq 0.89 \cdot (m+1).
\end{aligned}$$

This contradiction completes the proof of the claim. □

Write $\chi_x^k(t)$ and $\chi_y^k(t)$ for the indicator functions of the events $t \in G_x^k$ and $t \in G_y^k$, respectively.

Claim 2.6. *For each $k \in \mathbb{R}$,*

$$\mathbb{E}_T\left[\Pr[X_0 \in A_k \mid T] \cdot \Pr\left[Y_0 \in B_k \mid T\right] \cdot \chi_x^k(T) \cdot \chi_y^k(T)\right] \geq \tfrac{1}{10} \cdot \mathbb{E}_T\left[\Pr\left[X_0 \in A_k \mid T\right] \cdot \Pr\left[Y_0 \in B_k \mid T\right]\right].$$

Proof. Because $1 - \chi_x^k(t) \cdot \chi_y^k(t) \leq 1 - \chi_x^k(t) + 1 - \chi_y^k(t)$ holds for each t, and by linearity of expectation and symmetry, it suffices to prove that

$$\mathbb{E}_T\left[\Pr\left[X_0 \in A_k \mid T\right] \cdot \Pr\left[Y_0 \in B_k \mid T\right] \cdot \left(1 - \chi_x^k(T)\right)\right] \leq \tfrac{9}{20} \cdot \mathbb{E}_T\left[\Pr\left[X_0 \in A_k \mid T\right] \cdot \Pr\left[Y_0 \in B_k \mid T\right]\right].$$

To prove this, it in turn suffices to show that, for each *fixed* m-element subset $z_y \subset \{1, \ldots, \frac{n}{2}\}$, it holds that:

$$\begin{aligned}
&\mathbb{E}_T\left[\Pr\left[X_0 \in A_k \mid T\right] \cdot \Pr\left[Y_0 \in B_k \mid T\right] \cdot \left(1 - \chi_x^k(T)\right) \mid Z_y = z_y\right] \\
&\quad \leq \tfrac{9}{20} \cdot \mathbb{E}_T\left[\Pr\left[X_0 \in A_k \mid T\right] \cdot \Pr\left[Y_0 \in B_k \mid T\right] \mid Z_y = z_y\right].
\end{aligned}$$

We prove this latter claim in the following way:

$$\begin{aligned}
&\mathbb{E}_T\left[\Pr\left[X_0 \in A_k \mid T\right] \cdot \Pr\left[Y_0 \in B_k \mid T\right] \cdot \left(1 - \chi_x^k(T)\right) \mid Z_y = z_y\right] \\
&\quad = \Pr\left[Y_0 \in B_k \mid Z_y = z_y\right] \cdot \mathbb{E}_T\left[\Pr\left[X_0 \in A_k \mid T\right] \cdot \left(1 - \chi_x^k(T)\right) \mid Z_y = z_y\right] && \text{(by Claim 2.2)} \\
&\quad \leq \tfrac{25}{8} \cdot \Pr\left[Y_0 \in B_k \mid Z_y = z_y\right] \cdot \mathbb{E}_T\left[\Pr\left[X \in A_k \mid T\right] \cdot \left(1 - \chi_x^k(T)\right) \mid Z_y = z_y\right] && \text{(by Claim 2.3)} \\
&\quad = \tfrac{25}{8} \cdot \Pr\left[Y_0 \in B_k \mid Z_y = z_y\right] \cdot \Pr\left[X \in A_k \mid Z_y = z_y\right] \cdot \mathbb{E}_T\left[1 - \chi_x^k(T) \mid Z_y = z_y\right] && \text{(by Claim 2.2)} \\
&\quad \leq \tfrac{25}{8} \cdot \tfrac{1}{7} \cdot \Pr\left[Y_0 \in B_k \mid Z_y = z_y\right] \cdot \Pr\left[X \in A_k \mid Z_y = z_y\right] && \text{(by Claim 2.5)} \\
&\quad = \tfrac{25}{56} \cdot \Pr\left[Y_0 \in B_k \mid Z_y = z_y\right] \cdot \mathbb{E}_T\left[\Pr[X_0 \in A_k \mid T] \mid Z_y = z_y\right],
\end{aligned}$$

where the last equality holds because, conditioned on $Z_y = z_y$, the random sets X and X_0 have the same distribution. An additional application of Claim 2.2 completes the proof. □

Claim 2.7. $\sum_{k \in \mathbb{R}} \mathbb{E}_T\left[\Pr\left[X_0 \in A_k \mid T\right]\right] \leq 1$ *and* $\sum_{k \in \mathbb{R}} \mathbb{E}_T\left[\Pr\left[Y_0 \in B_k \mid T\right]\right] \leq 1$.

Proof. We prove the first inequality. Because the sets A_k—as k ranges throughout $\mathbb{R}$—are pairwise disjoint,

$$\sum_{k \in \mathbb{R}} \mathbb{E}_T\left[\Pr\left[X_0 \in A_k \mid T\right]\right] = \sum_{k \in \mathbb{R}} \Pr\left[X_0 \in A_k\right] \leq \Pr\Big[X_0 \in \bigcup_{k \in \mathbb{R}} A_k\Big].$$

This completes the proof. □

2.2 Completing the argument

We are now in a position to prove the lemma. Invoking finally the hypothesis whereby H is contained in D_n, we have that:

$$0 = \Pr[(X_1, Y_1) \in D_n] \geq \Pr[(X_1, Y_1) \in H].$$

Applying now the decomposition (1) we have:

$$0 = \Pr[(X_1, Y_1) \in H] \geq \sum_{k \in \mathbb{R}} \mathbb{E}_T \left[\Pr\left[X_1 \in A_k \mid T \right] \cdot \Pr\left[Y_1 \in B_k \mid T \right] \cdot \chi_x^k(T) \cdot \chi_y^k(T) \right].$$

Invoking Definition 2.4, we see further that:

$$0 \geq \sum_{k \in \mathbb{R}} \mathbb{E}_T \left[\left(\tfrac{1}{70} \cdot \Pr\left[X_0 \in A_k \mid T \right] - 2^{-\varepsilon \cdot n} \right) \cdot \left(\tfrac{1}{70} \cdot \Pr\left[Y_0 \in B_k \mid T \right] - 2^{-\varepsilon \cdot n} \right) \cdot \chi_x^k(T) \cdot \chi_y^k(T) \right].$$

Applying Claim 2.7, we have that:

$$0 \geq \tfrac{1}{70^2} \cdot \sum_{k \in \mathbb{R}} \mathbb{E}_T \left[\Pr\left[X_0 \in A_k \mid T \right] \cdot \Pr\left[Y_0 \in B_k \mid T \right] \cdot \chi_x^k(T) \cdot \chi_y^k(T) \right] - 2^{-\Omega(n)}.$$

Finally, using Claim 2.6, we conclude that:

$$\begin{aligned} 0 &\geq \tfrac{1}{10 \cdot 70^2} \cdot \sum_{k \in \mathbb{R}} \mathbb{E}_T \left[\Pr\left[X_0 \in A_k \mid T \right] \cdot \Pr\left[Y_0 \in B_k \mid T \right] \right] - 2^{-\Omega(n)} \\ &= \tfrac{1}{10 \cdot 70^2} \cdot \mathbb{E}_T \left[\sum_{k \in \mathbb{R}} \Pr\left[X_0 \in A_k \mid T \right] \cdot \Pr\left[Y_0 \in B_k \mid T \right] \right] - 2^{-\Omega(n)} \\ &= \tfrac{1}{10 \cdot 70^2} \cdot \mu_{\ell_x, \ell_y}(H) - 2^{-\Omega(n)}. \end{aligned}$$

This calculation completes the proof of the lemma.

References

[AF93] Noga Alon and Zoltán Füredi. Covering the cube by affine hyperplanes. *European Journal of Combinatorics*, 14(2):79–83, 1993.

[AGG$^+$21] James Aaronson, Carla Groenland, Andrzej Grzesik, Tom Johnston, and Bartłomiej Kielak. Exact hyperplane covers for subsets of the hypercube. *Discrete Mathematics*, 344(9), 2021.

[Dia21] Benjamin E. Diamond. Securely computing piecewise constant codes. `https://ia.cr/2021/146`, Oct 2021. To appear.

[Erd45] Paul Erdős. On a lemma of Littlewood and Offord. *Bulletin of the American Mathematical Society*, 51:898–902, 1945.

[FF88] Peter Frankl and Zoltán Füredi. Solution of the Littlewood–Offord problem in high dimensions. *Annals of Mathematics*, 128(2):259–270, 1988.

[Gri93] Jerrold R. Griggs. On the distribution of the sums of residues. *Bulletin of the American Mathematical Society*, 28(2):329–333, 1993.

[Kle65] Daniel J. Kleitman. On a lemma of Littlewood and Offord on the distribution of certain sums. *Mathematische Zeitschrift*, 90(4):251–259, 1965.

[LO43] John E. Littlewood and Cyril Offord. On the number of real roots of a random algebraic equation (III). *Sbornik: Mathematics*, 12(3):277–286, 1943.

[Raz92] Alexander A. Razborov. On the distributional complexity of disjointness. *Theoretical Computer Science*, 106(2):385–390, 1992.

[RY20] Anup Rao and Amir Yehudayoff. *Communication Complexity and Applications*. Cambridge University Press, 2020.