

Antichain codes

Benjamin Gunby, Xiaoyu He, Bhargav Narayanan, and Sam Spiro

ABSTRACT. A family of sets A is said to be an antichain if $x \not\subset y$ for all distinct $x, y \in A$, and it is said to be a distance- r code if every pair of distinct elements of A has Hamming distance at least r . Here, we prove that if $A \subset 2^{[n]}$ is both an antichain and a distance- r code, then $|A| = O_r(2^n n^{-1/2 - \lfloor (r-1)/2 \rfloor})$. This result, which is best-possible up to the implied constant, is a purely combinatorial strengthening of a number of results in Littlewood–Offord theory; for example, our result gives a short combinatorial proof of Hálász’s theorem, while all previously known proofs of this result are Fourier-analytic.

1. INTRODUCTION

In this paper, motivated by considerations from Littlewood–Offord theory, we study the intersection of two classical combinatorial problems in the hypercube, namely that of finding large antichains and that of finding large distance- r codes.

A family of sets $A \subset 2^{[n]}$ is an *antichain* if $x \not\subset y$ for any distinct $x, y \in A$. For example, the k -th layer

$$\binom{[n]}{k} = \{x \subset [n] : |x| = k\}$$

is an antichain for all $0 \leq k \leq n$, and it is a classical result of Sperner [11] that every antichain in the hypercube $2^{[n]}$ has size at most $\binom{n}{\lfloor n/2 \rfloor}$. There are a huge number of strengthenings and variants of Sperner’s theorem; we refer the reader to [2] for more background.

A family of vectors $B \subset \{0, 1\}^n$ is called a distance- r code if the Hamming distance between any pair of vectors in B is at least r ; identifying $\{0, 1\}^n$ and $2^{[n]}$ in the natural way, we call a family $A \subset 2^{[n]}$ a *distance- r code* if the symmetric difference $x \Delta y$ of any two distinct $x, y \in A$ has size at least r . One of the central problems of coding theory is to find large distance- r codes with various desirable properties, and the existence of such codes has many applications in both pure and applied problems. We refer the reader to [6] for more on coding theory, and mention only the basic fact (as evidenced by BCH codes) that the largest possible distance- r codes in $2^{[n]}$ have size $\Theta(2^n n^{-\lfloor (r-1)/2 \rfloor})$.

Date: 16 December, 2022.

2010 Mathematics Subject Classification. Primary 05D05; Secondary 68P30.

Here, we aim to answer the following natural question: how large can the cardinality of an *antichain code* in $2^{[n]}$ be? After some thought, one finds that it is difficult to do much better than taking the intersection of a large code and a large antichain; our main result shows that such constructions are indeed optimal.

Theorem 1.1. *For any fixed $r \in \mathbb{N}$, if $A \subset 2^{[n]}$ is both an antichain and a distance- r code, then*

$$|A| = O\left(2^n n^{-1/2 - \lfloor (r-1)/2 \rfloor}\right).$$

This result is best-possible up to multiplicative constants for antichain codes of any fixed distance, as we now explain.

Focusing first on codes of odd distance, we know (as discussed above) that for fixed $r \in \mathbb{N}$ and all large enough $n \in \mathbb{N}$, it is possible to construct a distance- $(2r + 1)$ code $A \subset 2^{[n]}$ with $|A| = \Theta(2^n n^{-r})$. By simple averaging, it is easy to show that there exists some $x \subset [n]$ for which $A \triangle x = \{a \triangle x : a \in A\}$, which is also a distance- $(2r + 1)$ code, intersects the $\lfloor n/2 \rfloor$ -th layer in at least

$$\Omega\left(\binom{n}{\lfloor n/2 \rfloor} n^{-r}\right) = \Omega\left(2^n n^{-1/2-r}\right)$$

sets; then $(A \triangle x) \cap \binom{[n]}{\lfloor n/2 \rfloor}$ gives us an antichain code whose size matches the bound in Theorem 1.1.

Turning next to codes of even distance, we note that if $A \subset 2^{[n]}$ is an antichain and a distance- $(2r + 1)$ code of cardinality $\Theta(2^n n^{-1/2-r})$ as constructed above, then by simple considerations of parity, either the even-sized elements of A or the odd-sized elements of A constitute an antichain and a distance- $(2r + 2)$ code of cardinality at least $|A|/2 = \Omega(2^n n^{-1/2-r})$, again matching the corresponding bound in Theorem 1.1.

As mentioned earlier, the primary motivation for Theorem 1.1 comes from the Littlewood–Offord theory of anti-concentration. In particular, Theorem 1.1 may be viewed as a purely combinatorial abstraction of an important result of Halász [7] that is widely used in the study of random matrices and random polynomials; see [5, 8] and the many references therein. To explain this connection, we need to fill in some background, a task to which we now turn.

Recall that the Littlewood–Offord problem asks the following: given a vector $\mathbf{a} = (a_1, \dots, a_n)$ of non-zero real numbers, estimate

$$\rho(\mathbf{a}) = \max_{\alpha \in \mathbb{R}} \mathbb{P}[\varepsilon_1 a_1 + \dots + \varepsilon_n a_n = \alpha],$$

where the ε_i 's are independent Bernoulli random variables with $\mathbb{P}[\varepsilon_i = 0] = \mathbb{P}[\varepsilon_i = 1]$. In their study of random polynomials, Littlewood and Offord [9] showed that $\rho(\mathbf{a}) = O(n^{-1/2} \log n)$ for any such \mathbf{a} , and soon after, Erdős [3] used Sperner's theorem to give a simple combinatorial proof of the sharp estimate $\rho(\mathbf{a}) \leq 2^{-n} \binom{n}{\lfloor n/2 \rfloor} = O(n^{-1/2})$.

There has since been considerable interest in establishing better bounds on $\rho(\mathbf{a})$ under stronger assumptions on the arithmetic structure of \mathbf{a} . For example, Erdős and Moser [4] proved that $\rho(\mathbf{a}) = O(n^{-3/2} \log n)$ whenever all of the entries of \mathbf{a} are distinct, Sárközy and Szemerédi [10] improved this to the asymptotically best-possible bound of $\rho(\mathbf{a}) = O(n^{-3/2})$, and Stanley [12] subsequently discovered how to deduce (very) sharp bounds for this problem from the hard Lefschetz theorem. Of particular interest to us is a far-reaching generalisation of the Sárközy–Szemerédi theorem due to Halász [7], one formulation of which is as follows.

Theorem 1.2. *Let $\mathbf{a} = (a_1, \dots, a_n)$ be a vector of real numbers with no linear relationships of complexity at most $2r$ between its entries, i.e., such that for any disjoint subsets $x, y \subset [n]$ with $|x| + |y| \leq 2r$, we have*

$$\sum_{i \in x} a_i \neq \sum_{j \in y} a_j.$$

Then, we have

$$\rho(\mathbf{a}) = O_r(n^{-1/2-r}).$$

Note in particular that the hypothesis in the result above in the $r = 1$ case is equivalent to saying that $a_i \neq a_j$ for any $i \neq j$, so the result in this case reduces to the Sárközy–Szemerédi theorem on the Erdős–Moser problem.

Halász’s theorem has since become a widely used tool in the study of random matrices and random polynomials. All known proofs of Halász’s theorem use some Fourier analysis, and are very much arithmetic in nature. While searching for an analogue of Halász’s theorem for some anti-concentration problems over the symmetric group, it became clear to us that it would be of some help to find a purely combinatorial proof of this result, in the spirit of Erdős’ classical approach. Arguably, the primary motivation for Theorem 1.1 is that Halász’s theorem is an easy corollary.

Proof of Theorem 1.2 assuming Theorem 1.1. We may start by assuming without loss of generality that $a_i > 0$ for all i ; this follows from noting that $\rho(\mathbf{a})$ is unaltered if we replace the 0/1-valued Bernoulli random variables in its definition with $-1/1$ -valued Rademacher random variables.

Now, fix any real number α and let A denote the family of subsets $x \subset [n]$ such that $\sum_{i \in x} a_i = \alpha$. First, note that A is an antichain. Indeed, having $x \subset y$ both in A would imply

$$\alpha = \sum_{i \in x} a_i < \sum_{i \in y} a_i = \alpha,$$

with the second inequality using $a_i > 0$ for all i . Next, observe that A is a distance- $(2r + 1)$ code. Indeed, for any distinct $x, y \in A$ we must have

$$\sum_{i \in x \setminus y} a_i = \sum_{j \in y \setminus x} a_j;$$

this implies, by the hypothesis on \mathbf{a} , that $|x \Delta y| = |x \setminus y| + |y \setminus x| > 2r$, as desired. Thus, we may apply Theorem 1.1 to A and conclude that the probability that $\varepsilon_1 a_1 + \dots + \varepsilon_n a_n = \alpha$ is $O_r(n^{-1/2-r})$; since this bound holds for any $\alpha \in \mathbb{R}$, we get the desired bound on $\rho(\mathbf{a})$. \square

Before we proceed, it is worth mentioning that there are more general forms of Halász's theorem that give bounds on $\rho(\mathbf{a})$ in terms of the *number of linear relationships of complexity at most $2r$* between the entries of \mathbf{a} (as opposed to the hypothesis that there are no such relationships, as in Theorem 1.2). Such statements may also be deduced from the proof of Theorem 1.1, albeit not directly from its statement. This involves bounding the cardinality of a family A that is *approximately* both an antichain and a distance- $(2r + 1)$ code; however, to avoid obscuring the ideas involved in the proof of Theorem 1.1, we do not pursue these generalisations in detail here. Since the relevant parts of the proof of Theorem 1.1 are based on (delicate but elementary) double counting, the modifications needed to establish such generalisations are not particularly involved, and we leave the details — with some hints appearing in the sequel — to the interested reader

Our proof of Theorem 1.1 relies on rather weak expansion properties of the Boolean lattice used in conjunction with some delicate double counting arguments (inspired by studying short random walks in the hypercube); this is presented, along with some motivating remarks, in Section 2. We close with a brief discussion of directions for subsequent work in Section 3.

2. PROOF OF THE MAIN RESULT

We start with some brief comments on notation. We adopt the convention that lower case letters (such as a, b, c, x, y, z) represent subsets of $[n]$, and that upper case letters (such as A, S) represent families of sets, i.e., subsets of $2^{[n]}$. If $S \subset 2^{[n]}$ and $r \geq 1$ is an integer, we write $\partial^r S$ for the r -fold shadow of S , i.e., the collection of sets which can be obtained by deleting r elements of $[n]$ from some set in S . Similarly, we write $\partial^{-r} S$ for the collection of sets which can be obtained by adding r elements to some set in S . For singletons we abuse notation by writing $\partial^r x$ for $\partial^r \{x\}$ and $\partial^{-r} x$ for $\partial^{-r} \{x\}$. Finally, we write $x \Delta y$ for the symmetric difference of x and y .

As we have already seen, we need only prove Theorem 1.1 for codes of odd distance; we state (and prove) this equivalent formulation below since this allows us to avoid cluttering the notation with floors and ceilings that are not crucial.

Theorem 2.1. *For any fixed $r \in \mathbb{N}$, if $A \subset 2^{[n]}$ is both an antichain and a distance- $(2r + 1)$ code, then*

$$|A| = O(2^n n^{-1/2-r}).$$

Before we state and prove the main lemma that drives the proof of Theorem 2.1, we recall one proof of Sperner's theorem that serves as our inspiration. The local-LYM inequality (see [1]) asserts that for any $S \subset \binom{[n]}{k}$, we have

$$|\partial S| \binom{n}{k-1}^{-1} \geq |S| \binom{n}{k}^{-1}.$$

It is not hard to show using local-LYM that any antichain $A \subset 2^{[n]}$ may be 'shifted', by means of taking shadows, into the middle layer without decreasing the size of the resulting family, whence we conclude that $|A| \leq \binom{n}{\lfloor n/2 \rfloor}$.

A natural approach to proving Theorem 2.1, say for antichain codes of distance 3 to be concrete, is to proceed along similar lines as above, except using the distance condition instead of the local-LYM inequality to generate more 'local expansion'. Concretely, given $A \subset 2^{[n]}$ that is both an antichain and a distance-3 code, it is easy to see for all k that $|\partial A_k| \geq k|A_k|$, where $A_k = A \cap \binom{[n]}{k}$; in particular, for $k \approx n/2$, this tells us that $|\partial A_k| \gtrsim n|A_k|/2$, which is a significant improvement over the rather modest bound $|\partial A_k| \gtrsim |A_k|$ promised by local-LYM. It is then natural to attempt to transform a given antichain code A of distance 3, by means of taking shadows, into a family that lives in the middle layer that is about n times larger, which would then show that $|A| \lesssim \binom{n}{\lfloor n/2 \rfloor} / n = O(2^n n^{-3/2})$, as desired.

To implement such an idea, we need to deal with how the shadows of the different A_k 's overlap as we repeatedly take shadows to move A into the middle layer. For example, an estimate of the following form would be ideal: for any $S \subset \binom{[n]}{k}$ disjoint from A_k (i.e., thinking of S as the shadow of all the A_ℓ 's with $\ell > k$ in layer k), we have $|\partial(S \cup A_k)| \geq |S| + k|A_k|/100$. Unfortunately, this is too much to hope for: if there are no conditions on the arbitrary set S , then it can be arranged so that ∂S contains the entirety of ∂A_k . Nevertheless, the following lemma shows that something like this ideal estimate does in fact hold when one studies the expansion of antichain codes over (slightly) longer ranges.

Lemma 2.2. *Let $n, r \geq 1$ be integers with $n \geq 8r$. If*

- (1) $S \subset \binom{[n]}{k}$,
- (2) $n/2 + 3r \leq k \leq 3n/4$, and
- (3) $A \subset \binom{[n]}{k-r} \setminus \partial^r S$ is a distance- $(2r + 1)$ code,

then

$$|\partial^{3r} S \cup \partial^{2r} A| \geq |S| + \frac{n^r |A|}{4(2r)^{3r}}.$$

Proof. Observe that because $k \geq n/2 + 3r$, local-LYM tells us that $|\partial B| \geq |B|$ for any family B inside one of the layers $\binom{[n]}{k}, \dots, \binom{[n]}{k-3r+1}$. As a result, there is nothing to prove when $A = \emptyset$, so let us assume that $A \neq \emptyset$. Let us also suppose for the sake of contradiction that $|\partial^{3r} S \cup \partial^{2r} A| < |S| + n^r |A| / 4(2r)^{3r}$.

Pick a uniformly random $a \in A$. Let b and b' denote a uniformly random pair of disjoint r -subsets of a , and c a uniformly random r -subset of $[n] \setminus a$. Note that since A is a distance- $(2r+1)$ code, $a \triangle b$ is a uniform random element of $\partial^r A$, and similarly, $a \triangle c$ is a uniform random element of $\partial^{-r} A$. Note also that a is uniquely determined by specifying either $a \triangle b$ or $a \triangle c$.

Claim 2.3. *The random element $a \triangle b$ of $\partial^r A$ satisfies*

$$\mathbb{P}[a \triangle b \notin \partial^{2r} S] < \frac{1}{4}.$$

Proof. By assumption,

$$\begin{aligned} |S| + \frac{n^r |A|}{4(2r)^{3r}} &> |\partial^{3r} S \cup \partial^{2r} A| \geq |\partial^{2r} S \cup \partial^r A| \\ &= |\partial^{2r} S| + |\partial^r A \setminus \partial^{2r} S| \\ &\geq |S| + |\partial^r A \setminus \partial^{2r} S|. \end{aligned}$$

Since A is a distance- $(2r+2)$ code in $\binom{[n]}{k-r}$ and $k-r \geq n/2$, we have

$$|\partial^r A| = \binom{k-r}{r} |A| \geq \left(\frac{k-r}{r}\right)^r |A| \geq \frac{n^r}{(2r)^r} |A| \geq \frac{n^r}{(2r)^{3r}} |A|.$$

Combining this with the inequality above gives

$$|\partial^r A \setminus \partial^{2r} S| < \frac{n^r |A|}{4(2r)^{3r}} \leq \frac{1}{4} |\partial^r A|.$$

This proves the claim since $a \triangle b$ is a uniform random element of $\partial^r A$. \square

Claim 2.4. *The random element $a \triangle (b \cup b' \cup c)$ of $\partial^{2r} \partial^{-r} A$ satisfies*

$$\mathbb{P}[a \triangle (b \cup b' \cup c) \in \partial^{2r} S] < \frac{1}{8}.$$

Proof. Let P be the set of pairs $(x, y) \in \partial^{-r} A \times \partial^{2r} S$ for which $y \in \partial^{2r} x$. There are a total of $\binom{n-k+2r}{2r} |\partial^{2r} S|$ ways of picking an element $y \in \partial^{2r} S$ and an element $x \in \partial^{-2r} y$, and of these ways at least $\binom{k}{2r} |S|$ satisfy $x \in S$. Since A is disjoint from $\partial^r S$, we have that $\partial^{-r} A$ is disjoint from S , so

$$\begin{aligned} |P| &\leq \binom{n-k+2r}{2r} |\partial^{2r} S| - \binom{k}{2r} |S| \\ &\leq \binom{n/2}{2r} (|\partial^{2r} S| - |S|) < \frac{n^{3r} |A|}{12 \cdot 2^r r^{3r} (2r)!}; \end{aligned}$$

here, the second inequality relies on $k \geq n/2 + 2r$ and $n/2 \geq 4r$, and the last inequality uses $\binom{n/2}{2r} \leq (n/2)^{2r}/(2r)!$ and $|\partial^{2r} S| \leq |\partial^{3r} S \cup \partial^{2r} A| < |S| + n^r |A|/4(2r)^{3r}$.

Also, observe that $a \triangle c$ is a uniform random element of $\partial^{-r} A$, so $a \triangle (b \cup b' \cup c) \in \partial^{2r} S$ if and only if $(a \triangle c, a \triangle (b \cup b' \cup c)) \in P$. Note that b, b', c are chosen uniformly at random out of

$$\binom{k-r}{r} \binom{k-2r}{r} \binom{n-k+r}{r} \geq \left(\frac{k-r}{r}\right)^r \left(\frac{k-2r}{r}\right)^r \left(\frac{n-k+r}{r}\right)^r \geq \frac{n^{3r}}{16^r r^{3r}} \quad (1)$$

possibilities, with the last inequality holding since both $k-2r \geq n/2$ and $k \leq 3n/4$. Since at most $(2r)!$ tuples (a, b, b', c) correspond to the same pair $(a \triangle c, a \triangle (b \cup b' \cup c))$ (as $a \triangle c$ determines a and c , the only non-injectivity comes from swapping elements between b, b'), we obtain

$$\mathbb{P}[a \triangle (b \cup b' \cup c) \in \partial^{2r} S] \leq \frac{(2r)!|P|}{|A| \cdot n^{3r}/16^r r^{3r}} < \frac{1}{4 \cdot 2^r} \leq \frac{1}{8}. \quad \square$$

We use these two claims to show that $\partial^{2r} S$ has large distance- $2r$ ‘edge expansion’ in $\binom{[n]}{k-2r}$.

Claim 2.5. *There are at least*

$$\frac{n^{3r}|A|}{2 \cdot 16^r r^{3r}}$$

pairs $(x, y) \in \binom{[n]}{k-2r}^2$ at distance $2r$ with $x \in \partial^{2r} S$ and $y \notin \partial^{2r} S$.

Proof. By the two previous claims, we have both $\mathbb{P}[a \triangle b \notin \partial^{2r} S] < 1/4$ and $\mathbb{P}[a \triangle (b \cup b' \cup c) \in \partial^{2r} S] < 1/8$. Thus, if we generate a random pair $(x, y) = (a \triangle b, a \triangle (b \cup b' \cup c))$, then x, y automatically have distance $2r$, and with probability at least $1 - 1/4 - 1/8 \geq 1/2$ they satisfy $x \in \partial^{2r} S$ and $y \notin \partial^{2r} S$. The total number of potential pairs (x, y) as above is

$$|\partial^r A| \binom{k-2r}{r} \binom{n-k-r}{r} = \binom{k-r}{r} |A| \cdot \binom{k-2r}{r} \binom{n-k-r}{r} \geq \frac{n^{3r}}{16^r r^{3r}} |A|,$$

with this last inequality using (1); we get the desired result by multiplying by $1/2$, i.e., the lower bound for the probability that both $x \in \partial^{2r} S$ and $y \notin \partial^{2r} S$. \square

We finish by enumerating in two ways the set Q of pairs $(y, z) \in \binom{[n]}{k-2r} \times \binom{[n]}{k-3r}$ where $z \in \partial^{3r} S$, $z \in \partial^r y$, and $y \notin \partial^{2r} S$. On the one hand, any pair (x, y) from the previous claim corresponds to such a pair $(y, z) \in Q$ by taking $z = x \cap y$, and this correspondence is at most $\binom{n-k+2r}{r}$ -to-one. By the previous claim,

$$|Q| \geq \frac{n^{3r}|A|}{2 \cdot 16^r r^{3r} \cdot \binom{n-k+2r}{r}} \geq \binom{n}{r}^{-1} \frac{n^{3r}|A|}{2 \cdot 16^r r^{3r}}.$$

On the other hand, the number of ways to pick z is $|\partial^{3r}S|$, the number of ways to pick $y \in \partial^{-r}z$ is $\binom{n-k+3r}{r}$, and of these pairs, at least $\binom{k-2r}{r}|\partial^{2r}S|$ satisfy $y \in \partial^{2r}S$. Thus,

$$\begin{aligned} |Q| &\leq \binom{n-k+3r}{r} |\partial^{3r}S| - \binom{k-2r}{r} |\partial^{2r}S| < \binom{n/2}{r} (|\partial^{3r}S| - |\partial^{2r}S|) \\ &\leq \binom{n/2}{r} (|\partial^{3r}S \cup \partial^{2r}A| - |S|) \leq \binom{n/2}{r} \frac{n^r |A|}{4(2r)^{3r}}. \end{aligned}$$

To get a contradiction, it suffices to show

$$\binom{n/2}{r} \binom{n}{r} < 2 \cdot 2^{-r} n^{2r},$$

which follows from $\binom{n/2}{r} \leq (n/2)^r$ and $\binom{n}{r} \leq n^r$. \square

Our main result follows quickly from Lemma 2.2.

Proof of Theorem 2.1. Recall that our goal is to prove that if $A \subset 2^{[n]}$ is both an antichain and a distance- $(2r+1)$ code for some fixed $r \geq 1$, then

$$|A| = O(2^n n^{-1/2-r}).$$

Let $A_k = A \cap \binom{[n]}{k}$ and let $S_k \subset \binom{[n]}{k}$ consist of the sets $x \subset [n]$ which are contained in some element of A . Since A is an antichain, we have $A_{k+2r} \subset \binom{[n]}{k+2r} \setminus \partial^r S_{k+3r}$. Additionally, since $S_k \supset \partial^{3r} S_{k+3r} \cup \partial^{2r} A_{k+2r}$, it follows from Lemma 2.2 that we have

$$|S_k| \geq |S_{k+3r}| + \frac{n^r |A_{k+2r}|}{4(2r)^{3r}}$$

for all $n/2 \leq k \leq 3n/4 - 3r$. By applying this bound inductively, we find for all $k \geq n/2$ that

$$|S_k| \geq \frac{n^r}{4(2r)^{3r}} \sum_{\ell \in L_k} |A_\ell|, \quad (2)$$

where L_k is the set of those $k \leq \ell \leq 3n/4 - 3r$ such that $\ell \equiv k + 2r \pmod{3r}$.

We now finish the proof by arguing that we may restrict our attention to a subset of the layers of the hypercube where the information supplied by (2) is easily utilised.

By decreasing the size of A by at most a factor of 2, we may assume $A_\ell = \emptyset$ for all $\ell < n/2$. Similarly, by decreasing the size of A by a factor of at most $3r$, we may assume there exists some i such that $A_\ell = \emptyset$ for all $\ell \not\equiv i \pmod{3r}$. Furthermore, observe that since A_ℓ is itself a distance- $(2r+1)$ code, every r -fold shadow $\partial^r x$ for $x \in A_\ell$ is a disjoint collection of $\binom{\ell}{r}$ sets in $\binom{[n]}{\ell-r}$. Hence, for each $n/2 \leq \ell \leq 3n/4$, we have $\binom{\ell}{r} |A_\ell| = O(2^n n^{-1/2})$, and consequently, $|A_\ell| = O(2^n n^{-1/2-r})$. Therefore, we may remove $\bigcup_{n/2 \leq \ell \leq n/2+3r} A_\ell$ from A and assume $A_\ell = \emptyset$ for all $n/2 \leq \ell \leq n/2 + 3r$. By standard estimates for the binomial coefficients, we have that $\sum_{\ell \geq 3n/4-3r} \binom{n}{\ell} \leq 1.9^n$ for

all sufficiently large $n \in \mathbb{N}$. Thus, if $k \geq n/2$ is the smallest integer with $k \equiv i - 2r \pmod{3r}$, the above assumptions and the bound (2) together imply that we have

$$\frac{n^r}{4(2r)^{3r}} (|A| - 1.9^n) \leq |S_k| \leq \binom{n}{k} = O(2^n n^{-1/2})$$

for all sufficiently large $n \in \mathbb{N}$; rearranging this gives us the desired bound on $|A|$ and completes the proof. \square

Finally, as mentioned earlier, it is possible to strengthen Theorem 1.2 to show that if there are at most Λn^r solutions to

$$\sum_{i \in x} a_i = \sum_{j \in y} a_j$$

amongst the entries of \mathbf{a} with x and y satisfying $\{|x| = |y| = r\} \wedge \{x \cap y = \emptyset\}$, then

$$\rho(\mathbf{a}) = O_r(\Lambda n^{-1/2-r}).$$

Such a result may also be established using our methods. To this end, we need a version of Lemma 2.2 where the assumption that A is an antichain is replaced by the assumption that there are at most Λn^r paths of length $2r$ going from A to $\partial^r A$ and back to A , and where our desired lower bound is one of the form $|S| + \Omega_r(n^r |A|/\Lambda)$.

The key to proving such a version of Lemma 2.2 is to note that the hypothesis implies that at least a $(99/100)$ -fraction of the length- r paths from A to $\partial^r A$ must reach elements of $\partial^r A$ lying below at most 100Λ elements of A ; let us write $\partial_{\leq 100\Lambda}^r A$ for the set of such elements. Now, an easy double counting argument may be used to show that

$$|\partial_{\leq 100\Lambda}^r A| = \Omega_r(n^r |A|/\Lambda).$$

We may define $\partial_{\leq 100\Lambda}^{-r} A$ analogously, and the rest of the argument proceeds essentially as before, but with these ‘robust’ shadow operators replacing the shadow operators ∂^r and ∂^{-r} .

3. CONCLUSION

To us, the most attractive feature of Theorem 1.1 is that the double counting arguments involved in its proof rely on rather weak expansion properties of the Boolean lattice (namely the local-LYM inequality), so we are optimistic that these techniques will apply elsewhere as well.

Concretely, we anticipate the techniques developed here to have some bearing on anti-concentration problems situated in posets where the Fourier-machinery needed for Halász’s theorem might be unavailable, but where some form of expansion is nonetheless available; we hope to revisit some of these problems (such as in the symmetric group, for example) in future work.

ACKNOWLEDGEMENTS

The second author was supported by the NSF grant DMS-2103154, the third author was supported by NSF grants CCF-1814409 and DMS-1800521, and the fourth author was supported by the NSF grant DMS-2202730. We are grateful to Noga Alon and Ross Berkowitz for stimulating conversations, and to Matthew Kwan for pointing out a small gap in an earlier draft of this paper.

REFERENCES

1. B. Bollobás, *Combinatorics*, Cambridge University Press, Cambridge, 1986. [5](#)
2. K. Engel, *Sperner theory*, Cambridge University Press, Cambridge, 1997. [1](#)
3. P. Erdős, *On a lemma of Littlewood and Offord*, Bull. Amer. Math. Soc. **51** (1945), 898–902. [2](#)
4. P. Erdős and L. Moser, *E736*, Amer. Math. Monthly **54** (1947), 229–230. [3](#)
5. A. Ferber, V. Jain, K. Luh, and W. Samotij, *On the counting problem in inverse Littlewood–Offord theory*, J. Lond. Math. Soc. (2) **103** (2021), 1333–1362. [2](#)
6. V. Guruswami, A. Rudra, and M. Sudan, *Essential coding theory*, (2012), [Link](#). [1](#)
7. G. Halász, *Estimates for the concentration function of combinatorial number theory and probability*, Period. Math. Hungar. **8** (1977), 197–211. [2](#), [3](#)
8. J. Kahn, J. Komlós, and E. Szemerédi, *On the probability that a random ± 1 -matrix is singular*, J. Amer. Math. Soc. **8** (1995), 223–240. [2](#)
9. J. E. Littlewood and A. C. Offord, *On the number of real roots of a random algebraic equation*, J. London Math. Soc. **13** (1938), 288–295. [2](#)
10. A. Sárközi and E. Szemerédi, *Über ein problem von Erdős und Moser*, Acta Arith. **11** (1965), 205–208. [3](#)
11. E. Sperner, *Ein satz über untermengen einer endlichen Menge*, Math. Z. **27** (1928), 544–548. [1](#)
12. R. P. Stanley, *Weyl groups, the hard Lefschetz theorem, and the Sperner property*, SIAM J. Algebraic Discrete Methods **1** (1980), 168–184. [3](#)

DEPARTMENT OF MATHEMATICS, RUTGERS UNIVERSITY, PISCATAWAY, NJ 08854, USA

Email address: bg570@connect.rutgers.edu

DEPARTMENT OF MATHEMATICS, PRINCETON UNIVERSITY, PRINCETON, NJ 08540, USA

Email address: xiaoyuh@princeton.edu

DEPARTMENT OF MATHEMATICS, RUTGERS UNIVERSITY, PISCATAWAY, NJ 08854, USA

Email address: narayanan@math.rutgers.edu

DEPARTMENT OF MATHEMATICS, RUTGERS UNIVERSITY, PISCATAWAY, NJ 08854, USA

Email address: sas703@scarletmail.rutgers.edu