Uniformly cross intersecting families

Noga Alon* Eyal Lubetzky †

October 18, 2008

Abstract

Let $\mathcal{A}$ and $\mathcal{B}$ denote two families of subsets of an n-element set. The pair $(\mathcal{A},\mathcal{B})$ is said to be ℓ-cross-intersecting iff $|A\cap B|=\ell$ for all $A\in\mathcal{A}$ and $B\in\mathcal{B}$. Denote by $P_\ell(n)$ the maximum value of $|\mathcal{A}||\mathcal{B}|$ over all such pairs. The best known upper bound on $P_\ell(n)$ is $\Theta(2^n)$, by Frankl and Rödl. For a lower bound, Ahlswede, Cai and Zhang showed, for all $n\geq 2\ell$, a simple construction of an ℓ-cross-intersecting pair $(\mathcal{A},\mathcal{B})$ with $|\mathcal{A}||\mathcal{B}|=\binom{2\ell}{\ell}2^{n-2\ell}=\Theta(2^n/\sqrt{\ell})$, and conjectured that this is best possible. Consequently, Sgall asked whether or not $P_\ell(n)$ decreases with ℓ.

In this paper, we confirm the above conjecture of Ahlswede et al. for any sufficiently large ℓ, implying a positive answer to the above question of Sgall as well. By analyzing the linear spaces of the characteristic vectors of $\mathcal{A},\mathcal{B}$ over $\mathbb{R}$, we show that there exists some $\ell_0>0$, such that $P_\ell(n)\leq\binom{2\ell}{\ell}2^{n-2\ell}$ for all $\ell\geq\ell_0$. Furthermore, we determine the precise structure of all the pairs of families which attain this maximum.

1 Introduction

Let $\mathcal{A}$ and $\mathcal{B}$ denote two families of subsets of an n-element set. We say that the pair $(\mathcal{A},\mathcal{B})$ is ℓ-cross-intersecting iff $|A\cap B|=\ell$ for all $A\in\mathcal{A}$ and $B\in\mathcal{B}$. Let $P_\ell(n)$ denote the maximum possible value of $|\mathcal{A}||\mathcal{B}|$ over all ℓ-cross-intersecting pairs $(\mathcal{A},\mathcal{B})$. We are interested in finding the precise value of $P_\ell(n)$, and in characterizing all the extremal pairs $\mathcal{A},\mathcal{B}$ which achieve this maximum.

The study of the maximal size of a single family of sets $\mathcal{F}\subset 2^{[n]}$, with specified pairwise intersections of its members, has received a considerable amount of attention over the years. For instance, the Erdős-Ko-Rado Theorem [6], one of the most fundamental theorems in Combinatorial Set Theory, gives a tight upper bound $|\mathcal{F}|\leq\binom{n-t}{k-t}$ in case $|F\cap F'|\geq t$ for all $F,F'\in\mathcal{F}$, $|F|=k$

*School of Mathematics, Institute for Advanced Study, Princeton, NJ 08540, USA, and Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, 69978, Israel. Email: nogaa@tau.ac.il. Research supported in part by the Israel Science Foundation, by a USA-Israel BSF grant, by NSF grant CCF 0832797 and by the Ambrose Monell Foundation.

†Theory Group of Microsoft Research, One Microsoft Way, Redmond, WA 98052-6399, USA. Email address: eyal@microsoft.com. Research partially supported by a Charles Clore Foundation Fellowship.

for all $F \in \mathcal{F}$ and n is sufficiently large. The case where there is no restriction on the size of the sets of $\mathcal{F}$ is treated by Katona's Theorem [11]. In both cases, there is a unique (up to a relabeling of the elements of $[n]$) family of sets which achieves the upper bound. For further results of this nature, see, e.g, [7], [8], [10], [15], as well as [3].

A well known conjecture of Erdős [5] stated that if $\mathcal{F} \subset 2^{[n]}$ is a family satisfying $|F \cap F'| \neq \lfloor \frac{n}{4} \rfloor$ for all $F, F' \in \mathcal{F}$, then $|\mathcal{F}| < (2-\varepsilon)^n$ for some $\varepsilon > 0$. This was proved by Frankl and Rödl [9], by considering the corresponding variant on two families: it is shown in [9], that if $\mathcal{A}, \mathcal{B} \subset 2^{[n]}$ and $|A \cap B| \neq l$, where $\eta n \leq l \leq (\frac{1}{2} - \eta)n$ for some $\eta < \frac{1}{4}$, then $|\mathcal{A}||\mathcal{B}| \leq (4 - \varepsilon(\eta))^n$. The authors of [9] studied several additional problems related to cross-intersections of two families of sets, and among their results, they provided the following upper bound on $P_\ell(n)$, which was later reproved in [1]:

$$\begin{cases} P_0(n) \leq 2^n \\ P_\ell(n) \leq 2^{n-1} \quad \text{for } \ell \geq 1 \end{cases} . \tag{1}$$

The argument which gives the upper bound of 2^n is simple: consider the characteristic vectors of the sets in $\mathcal{A}, \mathcal{B}$ as vectors in $\mathbb{Z}_2^n$. Notice that the intersection of two sets is equal to the inner product of the two corresponding vectors modulo 2. Therefore, if ℓ is even, then the families $\mathcal{A}, \mathcal{B}$ belong to two orthogonal linear spaces, giving $|\mathcal{A}||\mathcal{B}| \leq 2^n$. Otherwise, we may add an additional coordinate of 1 to all vectors, and repeat (carefully) the above argument, gaining a slight improvement: $|\mathcal{A}||\mathcal{B}| \leq 2^{n-1}$. Similar ideas are used to show that the upper bound 2^{n-1} holds for even values of $\ell > 0$ as well, by performing the analysis over $GF(p)$ for some prime $p > 2$ instead of over $\mathbb{Z}_2$.

As part of their study of questions in Coding Theory, Ahlswede, Cai and Zhang [1] gave the following simple construction of an ℓ-cross-intersecting pair: for $n \geq 2\ell$, let $\mathcal{A}$ contain a single 2ℓ-element set, A, and let $\mathcal{B}$ contain all the sets which contain precisely ℓ elements of A. This gives:

$$|\mathcal{A}||\mathcal{B}| = \binom{2\ell}{\ell} 2^{n-2\ell} = (1 + o(1)) \frac{2^n}{\sqrt{\pi \ell}} , \tag{2}$$

where the $o(1)$-term tends to 0 as $\ell \to \infty$. The upper bound (1) implies that this construction achieves the maximum of $P_\ell(n)$ for $\ell \in \{0, 1\}$, and the authors of [1] conjectured that this in fact holds for all ℓ.

As the upper bound (1) is independent of ℓ, compared to the above lower bound of $\Theta(2^n/\sqrt{\ell})$, Sgall [17] asked whether or not $P_\ell(n)$ is bounded from above by some decreasing function of ℓ. One of the motivations of [17] was a relation between problems of restricted cross-intersections of two families of sets and problems in Communication Complexity; see [17] for more details.

In [12], the authors verified the above conjecture of [1] for the case $\ell = 2$, by showing that $P_2(n) \leq 3 \cdot 2^{n-3}$. However, for any $\ell > 2$ the best known upper bound on $P_\ell(n)$ remained 2^{n-1}.

The following theorem confirms the above conjecture of [1] for all sufficiently large values of ℓ, and thus provides also a positive answer to the above question of Sgall.

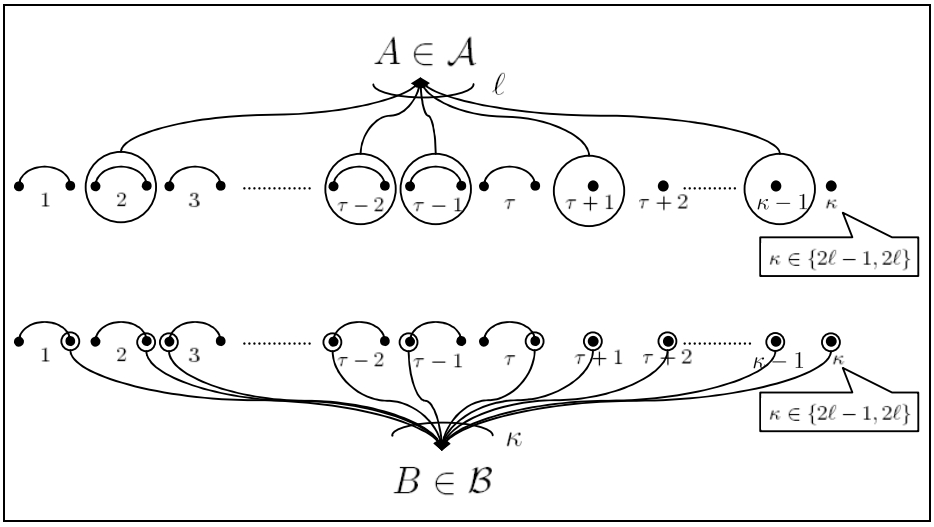

Figure 1: The extremal family (5) of ℓ-cross-intersecting pairs $\mathcal{A}, \mathcal{B}$ in case $n = \kappa + \tau$.

Theorem 1.1. *There exists some $\ell_0 > 0$ such that, for all $\ell \geq \ell_0$, every ℓ-cross-intersecting pair $\mathcal{A}, \mathcal{B} \subset 2^{[n]}$ satisfies:*

$$|\mathcal{A}||\mathcal{B}| \leq \binom{2\ell}{\ell} 2^{n-2\ell} \ . \tag{3}$$

Furthermore, if $|\mathcal{A}||\mathcal{B}| = \binom{2\ell}{\ell} 2^{n-\ell}$, then there exists some choice of parameters κ, τ, n':

$$\begin{aligned} &\kappa \in \{2\ell-1, 2\ell\} \ , \ \tau \in \{0, \ldots, \kappa\} \ , \\ &\kappa + \tau \leq n' \leq n, \end{aligned} \tag{4}$$

such that, up to a relabeling of the elements of $[n]$ and swapping $\mathcal{A}, \mathcal{B}$, the following holds:

$$\begin{aligned} \mathcal{A} \ &= \left\{ \bigcup_{T \in J} T \ : \ J \subset \left\{ \begin{array}{c} \{1, \kappa+1\}, \ldots, \{\tau, \kappa+\tau\}, \\ \{\tau+1\}, \ldots, \{\kappa\} \end{array} \right\} , \ |J| = \ell \right\} \times 2^X \ , \\ \mathcal{B} \ &= \left\{ L \cup \{\tau+1, \ldots, \kappa\} : \begin{array}{l} L \subset \{1, \ldots, \tau, \kappa+1, \ldots, \kappa+\tau\} \\ |L \cap \{i, \kappa+i\}| = 1 \text{ for all } i \in [\tau] \end{array} \right\} \times 2^Y \ . \end{aligned} \tag{5}$$

where $X = \{\kappa+\tau+1, \ldots, n'\}$ and $Y = \{n'+1, \ldots, n\}$.

An illustration of the family of extremal pairs $\mathcal{A}, \mathcal{B}$ described in Theorem 1.1 appears in Figure 1. Indeed, this family satisfies:

$$|\mathcal{A}||\mathcal{B}| = \binom{\kappa}{\ell} \cdot 2^{|X|} \cdot 2^{\tau+|Y|} = \binom{\kappa}{\ell} 2^{n-\kappa} = \binom{2\ell}{\ell} 2^{n-2\ell} \ ,$$

where the last inequality is by the choice of $\kappa \in \{2\ell-1, 2\ell\}$. The construction of [1] fits the special case $\tau = 0$, $\kappa = 2\ell$.

The proof of Theorem 1.1 combines tools from linear algebra with techniques from extremal combinatorics, including the Littlewood-Offord Lemma, extensions of Sperner's Theorem and some large deviation estimates.

The rest of this paper is organized as follows: Section 2 includes some of the ingredients needed for the proof of Theorem 1.1. In order to prove the main result, we first prove a weaker version of Theorem 1.1, which states that $P_\ell(n) \leq 2^{n+3}/\sqrt{\ell}$ for every sufficiently large ℓ (note that this result alone gives a positive answer to the above question of Sgall). This is shown in Section 3. In Section 4 we reduce the proof of Theorem 1.1 to two lemmas, Lemma 4.1 and Lemma 4.2. These lemmas are proved in Sections 5 and 6 respectively. Section 7 contains some concluding remarks and open problems.

Throughout the paper, all logarithms are in base 2.

2 Preliminary Sperner-type Theorems

2.1 Sperner's Theorem and the Littlewood-Offord Lemma

If P is a finite partially ordered set, an antichain of P is a set of pairwise incomparable elements. Sperner's Theorem [18] provides a tight upper bound on the maximal size of an antichain, when P is the collection of all subsets of an n-element set with the subset relation ($A \leq B$ iff $A \subset B$):

Theorem 2.1 ([18]). *If $\mathcal{A}$ is an antichain of an n-element set, then $|\mathcal{A}| \leq \binom{n}{\lfloor n/2 \rfloor}$.*

In [13], Littlewood and Offord studied a problem which has the following formulation in the 1-dimensional case: let $a_1, \ldots, a_n \in \mathbb{R}$ with $|a_i| > 1$ for all i. What is the maximal number of sub-sums $\sum_{i \in I} a_i$, $I \subset [n]$, which lie in an interval of length 1? An immediate lower bound is $\binom{n}{\lfloor n/2 \rfloor}$, when, for some $\alpha > 1$, half of the a_i-s is equal to α and the other half is equal to $-\alpha$.

Using Sperner's Theorem, Erdős [4] gave a tight upper bound of $\binom{n}{\lfloor n/2 \rfloor}$ for the 1-dimensional case of the so-called Littlewood-Offord Lemma. To see this, consider the maximal number of sub-sums of $a_1, \ldots, a_n$, which all belong to some unit interval. Without loss of generality, we may assume that all the a_i-s are positive (possibly shifting the target unit interval). Therefore, $a_i > 1$ for all i, implying that the desired family of subsets is an antichain. The result now follows from Sperner's Theorem. Using a similar argument, Erdős proved the following stronger result:

Lemma 2.2 ([4]). *Let $a_1, \ldots, a_n \in \mathbb{R} \setminus \{0\}$, and let $\delta = \min\{|a_i|\}$. Let T be a union of m half-open intervals, each of width at most δ. Then the number of sub-sums $\sum_{i \in I} a_i$, $I \subset [n]$, which belong to T, is at most the sum of the m middle binomial coefficients in n.*

2.2 A bipartite extension of Sperner's Theorem

The following lemma gives an upper bound on the size of an antichain of $[n]$, which satisfies an additional requirement with respect to a pre-defined partition of $[n]$ into two sets.

Lemma 2.3. *Let $U = [u]$ and $V = [n] \setminus U$, $u \leq n$. If $\mathcal{A}$ is an antichain of $[n]$, and in addition satisfies: $|A \cap V| = f(|A \cap U|)$ for all $A \in \mathcal{A}$, where $f : \mathbb{N} \to \mathbb{N}$ is some monotone increasing function, then $|\mathcal{A}| \leq \binom{u}{\lfloor u/2 \rfloor}\binom{n-u}{\lfloor (n-u)/2 \rfloor}$.*

The above lemma will follow from the next generalization of Sperner's Theorem:

Proposition 2.4. *Let $U = [u]$ and $V = [n] \setminus U$, $u \leq n$. If every two sets $A \neq B \in \mathcal{A}$ satisfy that either $A \cap U$, $B \cap U$ are incomparable or $A \cap V$, $B \cap V$ are incomparable, then $|\mathcal{A}| \leq \binom{u}{\lfloor u/2 \rfloor}\binom{n-u}{\lfloor (n-u)/2 \rfloor}$.*

Proof. Notice that the upper bound is tight, as it is achieved by a cartesian product of maximal antichains of U and V. The proof is based on Lubbell's proof [14] of Sperner's Theorem and the LYM inequality. For each $A \in \mathcal{A}$, let:

$$A_U = A \cap U \ , \ A_V = \{x - u : x \in A \cap V\} \ . \tag{6}$$

Let $\sigma \in S_u$ and $\pi \in S_{n-u}$ (where S_m is the symmetric group on m elements) denote two random permutations, chosen uniformly and independently . We define the event E_A for $A \in \mathcal{A}$ to be:

$$E_A = (\ A_U = \{\sigma(1), \ldots, \sigma(|A_U|)\} \ \wedge \ A_V = \{\pi(1), \ldots, \pi(|A_V|)\}\ ) \ ,$$

that is, the first entries of σ form A_U, and the first entries of π form A_V. The key observation is that the events E_A and E_B are disjoint for all $A \neq B \in \mathcal{A}$. To see this, assume that $E_A \wedge E_B$ holds for some $A \neq B \in \mathcal{A}$. The fact that the first entries of σ form both A_U and B_U implies that either $A_U \subset B_U$ or $B_U \subset A_U$, and the same applies to A_V, B_V. Therefore, the assumption on $\mathcal{A}$ implies that the events E_A and E_B are indeed disjoint, and thus:

$$\sum_{A \in \mathcal{A}} \Pr[E_A] = \Pr[\bigcup_{A \in \mathcal{A}} E_A] \leq 1 \ .$$

Since:

$$\Pr[E_A] = \frac{1}{\binom{u}{|A_U|}\binom{n-u}{|A_V|}} \ ,$$

it follows that:

$$\sum_{A \in \mathcal{A}} \frac{1}{\binom{u}{|A_U|}\binom{n-u}{|A_V|}} \leq 1 \ . \tag{7}$$

Note that in the special case $u = n$ this is the LYM inequality. The left hand side of (7) is at most $\sum_{A \in \mathcal{A}} 1/\left(\binom{u}{\lfloor u/2 \rfloor}\binom{n-u}{\lfloor (n-u)/2 \rfloor}\right)$ and the desired result follows. ■

Proof of Lemma 2.3. Following the notation of Proposition 2.4, define A_U and A_V for each $A \in \mathcal{A}$ as in (6). By Proposition 2.4, it suffices to show that, for all $A \neq B \in \mathcal{A}$, either A_U, B_U are incomparable or A_V, B_V are incomparable. Assume the contrary, and let $A \neq B \in \mathcal{A}$ be a counterexample. Without loss of generality, assume that $A_U \subset B_U$. If $A_V \subset B_V$ then $A \subset B$, contradicting the fact that $\mathcal{A}$ is an antichain. It follows that $B_V \subsetneqq A_V$, and since f is monotone increasing, the following holds:

$$|A_V| > |B_V| = f(|B_U|) \geq f(|A_U|) \ ,$$

contradicting the assumption that $|A_V| = f(|A_U|)$. ■

3 An upper bound tight up to a constant

In this section we prove a weaker version of Theorem 1.1, whose arguments will be later extended to prove the precise lower bound.

Theorem 3.1. *For any sufficiently large $\ell \in \mathbb{N}$, every ℓ-cross-intersecting pair $\mathcal{A}, \mathcal{B} \subset 2^{[n]}$ satisfies:*

$$|\mathcal{A}||\mathcal{B}| \leq \frac{2^{n+3}}{\sqrt{\ell}} \ . \tag{8}$$

Proof. Let $\mathcal{A}$ and $\mathcal{B}$ be as above. A key observation is the following: it is sufficient to prove (8) for the case where both $\mathcal{A}$ and $\mathcal{B}$ are antichains. This follows from an induction on n, where in the case $n = \ell$, $|\mathcal{A}||\mathcal{B}| = 1$ and (8) clearly holds. Indeed, suppose that there exist $A_1, A_2 \in \mathcal{A}$ such that $A_1 \subset A_2$. As $(\mathcal{A}, \mathcal{B})$ are ℓ-cross-intersecting, this implies that:

$$B \cap (A_2 \setminus A_1) = \emptyset \text{ for all } B \in \mathcal{B} \ , \tag{9}$$

hence the restriction of the families $(\mathcal{A}, \mathcal{B})$ to $[n] \setminus (A_2 \setminus A_1)$, $(\mathcal{A}', \mathcal{B}')$, is an ℓ-cross-intersecting pair of an n'-element set, where $n' < n$. By (9), $|\mathcal{B}'| = |\mathcal{B}|$, and by the induction hypothesis:

$$|\mathcal{A}||\mathcal{B}| \leq 2^{n-n'}|\mathcal{A}'||\mathcal{B}'| \leq \frac{2^{n+3}}{\sqrt{\ell}} \ ,$$

as required.

For any subset $A \subset [n]$, let $\chi_A \in \{0,1\}^n$ denote its characteristic vector. Let $\mathcal{F}_\mathcal{A}$ and $\mathcal{F}_\mathcal{B}$ denote the linear subspaces of $\mathbb{R}^n$ formed by the characteristic vectors of $\mathcal{A}$ and $\mathcal{B}$ respectively:

$$\begin{array}{rcl} \mathcal{F}_\mathcal{A} & = & \mathrm{span}(\{\chi_A : A \in \mathcal{A}\}) \subset \mathbb{R}^n \ , \\ \mathcal{F}_\mathcal{B} & = & \mathrm{span}(\{\chi_B : B \in \mathcal{B}\}) \subset \mathbb{R}^n \ , \end{array} \tag{10}$$

and assume without loss of generality that $\dim(\mathcal{F}_\mathcal{A}) \geq \dim(\mathcal{F}_\mathcal{B})$. Choose an arbitrary set $B_1 \in \mathcal{B}$ and define:

$$\begin{array}{l} \mathcal{F}'_\mathcal{B} = \mathrm{span}(\{\chi_B - \chi_{B_1} : B \in \mathcal{B}\}) \ , \\ k = \dim(\mathcal{F}_\mathcal{A}) \ , \ h = \dim(\mathcal{F}'_\mathcal{B}) \leq \dim(\mathcal{F}_\mathcal{B}) \ . \end{array} \tag{11}$$

By the definition of ℓ-cross-intersection, it follows that $\mathcal{F}_\mathcal{A}, \mathcal{F}'_\mathcal{B}$ are two orthogonal linear subspaces of $\mathbb{R}^n$, and $k + h \leq n$. Note also that $k \geq h$ by the assumption on $\dim(\mathcal{F}_\mathcal{A})$.

Let $M_\mathcal{A}$ denote the $k \times n$ row-reduced echelon form matrix, which is the result of performing Gauss elimination on the row-vectors $\{\chi_A : A \in \mathcal{A}\}$ over $\mathbb{R}$, and let $M_\mathcal{B}$ denote the corresponding $h \times n$ matrix for the vectors $\{\chi_B - \chi_{B_1} : B \in \mathcal{B}\}$. As $\mathrm{rank} M_\mathcal{A} = k$ and $\mathrm{rank} M_\mathcal{B} = h$, without loss of generality we have:

$$M_\mathcal{A} = \left(\begin{array}{c|c} I_k & * \end{array} \right) \ , \ M_\mathcal{B} = \left(\begin{array}{c|c} I_h & * \end{array} \right) \ .$$

where I_r denotes the identity matrix of order r (and the order of the columns in $M_\mathcal{A}$ and $M_\mathcal{B}$ is not necessarily the same). This implies that any linear combination of the rows of $M_\mathcal{A}$ which belongs

to $\{0,1\}^n$ has precisely two possible coefficients for each row: $\{0,1\}$, and in particular, $|\mathcal{A}| \leq 2^k$. Similarly, $|\mathcal{B}| \leq 2^h$ (the two possible coefficients in the affine combination are now determined by the vector χ_{B_1}), hence $|\mathcal{A}||\mathcal{B}| \leq 2^{k+h} \leq 2^n$, giving the known upper bound of [9]. Observe that if $k + h \leq n - \log n$, we get

$$|\mathcal{A}||\mathcal{B}| \leq \frac{2^n}{n} ,$$

and (8) clearly holds. Therefore, recalling that $k \geq h$, we may assume that:

$$\begin{cases} \frac{n}{2} - \frac{1}{2}\log n < & k \\ n - \log n < & k+h \quad \leq n \end{cases} . \tag{12}$$

We claim that the following statement, which clearly implies (8), holds:

$$|\mathcal{A}||\mathcal{B}| \leq \frac{2^{k+h+3}}{\sqrt{n}}. \tag{13}$$

To show this, we need the next lemma, which will be applied once on $M_{\mathcal{A}}, \mathcal{A}, k$ and once on $M_{\mathcal{B}}, \mathcal{B}, h$, to conclude that a constant fraction of the rows of $M_{\mathcal{A}}$ and $M_{\mathcal{B}}$ have precisely two non-zero entries, 1 and -1.

Lemma 3.2. *Let M denote a $d \times n$ matrix in row-reduced echelon form: $M = \left(\begin{array}{c|c} I_d & * \end{array} \right)$, and let $\mathcal{D}$ denote an antichain of subsets of $[n]$. Assume that:*

1. *The characteristic vectors of $\mathcal{D}$ belong to $w + \mathrm{span}(M)$, the affine subspace formed by some fixed vector $w \in \{0,1\}^n$ and the span of the rows of M.*
2. *The antichain $\mathcal{D}$ satisfies $|\mathcal{D}| \geq 8 \cdot 2^d/\sqrt{n}$.*

Then there exists a subset of c rows of M, $C \subset [d]$, where $c \geq d - \frac{n}{20} - 10\log n$, such that:

1. *Every row i of C belongs to $\{0, \pm 1\}^n \setminus \{0,1\}^n$.*
2. *Every column of the $c \times n$ sub-matrix formed by C contains at most 1 non-zero entry.*

Proof. Our first step is to remove a small portion of the rows of M, such that the remaining rows will have at most one non-zero entry in each column.

Claim 3.3. *Let $M, \mathcal{D}, w$ satisfy the requirements of Lemma 3.2. There exists a set of rows $R \subset [d]$ such that $|R| \leq \frac{n}{25} + 10\log n$, and each column of M has at most one non-zero value in the remaining $d - |R|$ rows.*

Proof of Claim. Perform the following process of column-selection on M: first, set $M' = M$. If M' has no column with at least 2 non-zero entries, the process ends. Otherwise, perform the following step (step j, for $j \geq 1$):

- Let i_j denote the index of a column of M' with a maximal number of non-zero entries, r_j.

- Let R_j denote the set of rows where the column i_j is non-zero ($|R_j| = r_j$).
- Replace all these rows in M' by 0-rows, and continue the process.

The result is a sequence of indices, $i_1, \ldots, i_t$ ($t \geq 0$) and a sequence of sets of rows $R_1, \ldots, R_t$ of sizes $r_1 \geq r_2 \geq \ldots \geq r_t > 1$, such that the column i_j has r_j non-zero values in the rows R_j, and $R_j \cap R_{j'} = \emptyset$ for all $j \neq j'$. Finally, the sub-matrix formed by removing the rows $R = \cup_{j=1}^{t} R_j$ from M has at most 1 non-zero entry in every column.

Consider affine combinations (with the affine vector w) of the rows of M which produce a $\{0,1\}^n$-vector. As stated above, each row of M allows precisely two coefficients in such an affine combination, as the first d columns of M form the identity matrix. Clearly, the value of the affine combination at index i_1 depends precisely on the r_1 coefficients of the rows R_1. In general, if we already chose the coefficients for the rows $\cup_{j'<j} R_{j'}$, then the value of the affine combination at index i_j depends only on the choice of the r_j coefficients for the rows R_j.

A simple argument will show that for $1 \leq j \leq t$, at most $\frac{3}{4}$ of the above 2^{r_j} combinations of coefficients for the rows R_j are indeed valid. To this end, recall the following simple fact, which corresponds to the Cauchy-Davenport Theorem when A, B are subsets of $\mathbb{Z}/p\mathbb{Z}$ instead of $\mathbb{R}$:

$$|A+B| \geq |A| + |B| - 1 \quad \text{for any two finite nonempty } A, B \subset \mathbb{R} \ , \tag{14}$$

where $A + B = \{a + b : a \in A,\ b \in B\}$. To see this, simply sort the values of A and B by order of magnitude, then produce distinct sums by iterating first on A, then on B.

Suppose we already chose coefficients for the rows $\cup_{j'<j} R_{j'}$, and consider the column i_j. Select 2 arbitrary rows $u, v \in R_j$, and fix the choice of coefficients for the remaining $r_j - 2$ rows. We are left with a choice between two coefficients for u, yielding two possible values a_1, a_2 contributed by u to the index i_j. Similarly, the row v contributes one of two possible values b_1, b_2 to the index i_j. Setting $A = \{a_1, a_2\}$ and $B = \{b_1, b_2\}$, the above fact implies that $|A + B| \geq 3$, hence at least one of the 4 possible combinations of u and v gives a non-$\{0,1\}$ value in index i_j of the resulting affine combination. Therefore, at most $\frac{3}{4}$ of the 2^{r_j} combinations for R_j result in a $\{0,1\}^n$ vector. We conclude that $|\mathcal{D}| \leq \left(\frac{3}{4}\right)^t 2^d$, and hence $t \leq 2 \log n$, otherwise we would get:

$$|\mathcal{D}| \leq \frac{2^d}{n^{2\log(4/3)}} < \frac{2^d}{\sqrt{n}} \ ,$$

contradicting the assumption on $|\mathcal{D}|$.

After providing an upper bound on t, we wish to bound the term $\sum_{i=1}^{t} r_i$. Let $0 \leq s \leq t$ denote the maximal index such that $r_s \geq 6$, that is:

$$r_1 \geq r_2 \geq \ldots \geq r_s \geq 6 \ ,$$
$$6 > r_{s+1} \geq r_{s+2} \geq \ldots \geq r_t > 1 \ .$$

As before, we consider the choice of coefficients for the rows R_j at step j, determining the i_j-th entry of the linear combination. By the Littlewood-Offord Lemma (Lemma 2.2), we conclude that

there are at most $2\binom{r_j}{\lfloor r_j/2 \rfloor} < \frac{2}{\sqrt{\frac{\pi}{2} r_j}} 2^{r_j}$ possible combinations of the rows R_j which yield a $\{0,1\}$-value in the i_j column (note that the inequality $\binom{2x}{x} \leq 2^{2x}/\sqrt{\pi x}$ holds for every integer $x \geq 1$, by the improved approximation [16] of the error term in Stirling's formula). Applying this argument to $i_1, \ldots, i_s$, we obtain that:

$$|\mathcal{D}| \leq 2^d \prod_{i=1}^{s} \frac{2\sqrt{2/\pi}}{\sqrt{r_i}} \ . \tag{15}$$

Observe that every m reals $a_1, \ldots, a_m \geq 2$ satisfy:

$$\prod_{i=1}^{m} \frac{1}{a_i} \leq \frac{1}{\sum_{i=1}^{m} a_i}$$

(this follows by induction on m from the fact that $xy \geq x + y$ for $x, y \geq 2$). Therefore, as $r_i \geq 6 > 2 \cdot (2\sqrt{2/\pi})^2$ for $1 \leq i \leq s$, it follows that:

$$\prod_{i=1}^{s} \frac{2\sqrt{2/\pi}}{\sqrt{r_i}} = \Big[\prod_{i=1}^{s} \frac{1}{r_i/(2\sqrt{2/\pi})^2} \Big]^{1/2} \leq \frac{2\sqrt{2/\pi}}{\sqrt{\sum_{i=1}^{s} r_i}} \ .$$

Combining this with (15) we obtain that if $\sum_{i=1}^{s} r_i > n/25$, then $|\mathcal{D}| < 8 \cdot 2^d/\sqrt{n}$, contradicting the assumption on $|\mathcal{D}|$. Assume therefore that $\sum_{i=1}^{s} r_i \leq n/25$. Altogether, we obtain that $R = \cup_{j=1}^{t} R_j$ satisfies:

$$|R| = \sum_{i=1}^{t} r_i \leq (\sum_{i=1}^{s} r_i) + 5(t-s) \leq \frac{n}{25} + 10 \log n \ .$$

This completes the proof of the claim. ■

It remains to deal with rows which do not belong to $\{0, \pm 1\}^n \setminus \{0,1\}^n$. The next claim provides an upper bound on the number of such rows in M:

Claim 3.4. *Let $M, \mathcal{D}, w$ satisfy the requirements of Lemma 3.2, and let $R \subset [d]$ be a set of indices of rows of M as provided by Claim 3.3. Let S denote the set of indices in $[d] \setminus R$ of rows which do not belong to $\{0, \pm 1\}^n \setminus \{0,1\}^n$. Then $|S| < n/100$.*

Proof of Claim. To prove the claim, fix a linear combination u of the rows $[d] \setminus S$, and consider all the possible combinations of the rows of S which can be added to $w' = w + u$ to produce vectors of $\mathcal{D}$. We will show that the number of these combinations is at most $2^s/\sqrt{\pi s/2}$, where $s = |S|$, and the result will follow from the assumption on $|\mathcal{D}|$.

Put $S = S_{01} \cup S_{\overline{01}}$, where $S_{01} \subset S$ is the set of indices of rows in S which are $\{0,1\}^n$ vectors, and $S_{\overline{01}} = S \setminus S_{01}$. Recall that the first d columns of M form the identity matrix, and that $w \in \{0,1\}^n$, hence the only two coefficients which can be assigned to the row i to produce $\{0,1\}$ values in the i-th column are:

$$\begin{cases} \{0,1\} & \text{if } w_i = 0 \\ \{0,-1\} & \text{if } w_i = 1 \end{cases} \ . \tag{16}$$

It will be more convenient to have the coefficients $\{0,1\}$ for all rows of S: to obtain this, subtract each row $i \in S$, whose coefficients are $\{0,-1\}$, from w', and let w'' denote the resulting vector.

Let $i \in S_{\overline{01}}$ be an index of a row which does not belong to $\{0,\pm 1\}^n$, and let j denote a column such that $M_{ij} = \lambda \notin \{0,\pm 1\}$. Crucially, $S \cap R = \emptyset$, hence column j contains at most one non-zero entry in the rows of S. Therefore, the two possible values of the affine combination in index j are $\{w''_j, w''_j + \lambda\}$, and as $0 < |\lambda| \neq 1$ it follows that at least one of these values does not belong to $\{0,1\}$. We deduce that there is at most one valid choice of coefficients for all the rows $S_{\overline{01}}$. Denoting this unique combination of the rows of $S_{\overline{01}}$ by v, it follows that every linear combination of S which, when added to w', belongs to $\mathcal{D}$, is the sum of $z = w'' + v$ and a linear combination of S_{01}.

It remains to set the coefficients of the rows S_{01}, and since each row of S_{01} has $\{0,1\}$ as its coefficients, we are considering a sum of a subset of the rows of S_{01}. Each of these rows belongs to $\{0,1\}^n$, and in particular, is non-negative: we claim that the set of possible subsets of S_{01} is therefore an antichain. To see this, suppose that two distinct subsets $X, Y \subset S_{01}$, $X \subset Y$, produce (when added to z) two vectors $x, y \in \mathbb{R}^n$ which correspond to sets in $\mathcal{D}$. The values of x, y at the indices of S_{01} are determined by the sets X, Y (in fact, these values are equal to those of the corresponding characteristic vectors), hence $x \neq y$. Furthermore, as the rows of S_{01} are non-negative, and $X \subset Y$, we have $x_i \leq y_i$ for all $i \in [n]$. This contradicts the fact that $\mathcal{D}$ is an antichain. Let $s' = |S_{01}|$; Sperner's Theorem gives:

$$|\mathcal{D}| \leq 2^{d-s} \cdot \binom{s'}{\lfloor s'/2 \rfloor} \leq 2^{d-s} \cdot \binom{s}{\lfloor s/2 \rfloor} \leq \frac{2^d}{\sqrt{\pi s/2}} \ ,$$

and by the assumption on $|\mathcal{D}|$, we obtain that $s \leq n/100$, completing the proof of the claim. ■

Altogether, Claims 3.3 and 3.4 imply that we can delete at most

$$|R| + |S| \leq \frac{n}{20} + 10 \log n$$

rows of M, and obtain a subset of c rows, $d - \frac{n}{20} - 10 \log n \leq c \leq d$, satisfying the statements of the lemma. ■

Note that the requirements of Lemma 3.2 are satisfied both by $M_{\mathcal{A}}, \mathcal{A}$ and by $M_{\mathcal{B}}, \mathcal{B}$. Indeed, if either $|\mathcal{A}| < \frac{8}{\sqrt{n}} \cdot 2^k$ or $|\mathcal{B}| < \frac{8}{\sqrt{n}} \cdot 2^h$, then (13) holds and we are done. The remaining requirement on the characteristic vectors of $\mathcal{D}$ is satisfied by definition (for $\mathcal{A}$, w is the zero vector, whereas for $\mathcal{B}$, $w = \chi_{B_1}$).

Applying Lemma 3.2 to $M_{\mathcal{A}}, \mathcal{A}$, we obtain a set of at least $c_1 \geq k - \frac{n}{20} - 10 \log n$ rows, $C_1 \subset [k]$, such that each row has an entry of -1 at some index $j > k$, and each column has at most 1 non-zero entry in these rows. In particular, we get: $c_1 \leq n - k$, and thus:

$$k - \frac{n}{20} - 10 \log n \leq n - k \ ,$$

and by (12) we get:

$$\begin{cases} \frac{n}{2} - \log n & \leq k \leq \frac{21}{40}n + 5\log n \\ \frac{19}{40}n - 6\log n & \leq h \leq \frac{n}{2} \end{cases} . \tag{17}$$

Next, let $C_1' \subset C_1$ denote the set of indices of rows of C_1 with precisely two non-zero entries. Notice that, as each of the columns $\{k+1, \ldots, n\}$ contains at most 1 non-zero entry in the rows C_1, and on the other hand, each of the rows C_1 contains a non-zero value in one of these columns, it follows that $|C_1 \setminus C_1'| \leq n - k - c_1$. The lower bound on c_1 and (17) give the following bound on $c_1' = |C_1'|$:

$$c_1' \geq c_1 - (n - k - c_1) \geq 3k - \frac{n}{10} - 20\log n - n \geq \frac{2}{5}n - 23\log n \ . \tag{18}$$

Since each row $i \in C_1'$ has precisely 2 non-zero entries, it follows that it has the entry 1 at index i and the entry -1 at some index $j > k$.

Applying Lemma 3.2 to $M_{\mathcal{B}}$ and $\mathcal{B}$, we obtain a set of at least $c_2 \geq h - \frac{n}{20} - 10\log n$ rows, $C_2 \subset [h]$, and a similar argument to the one above implies that at most $n - h - c_2$ rows can contain more than 2 non-zero entries. Let $C_2' \subset C_2$ denote the set indices of rows of C_2 with precisely two non-zero entries, and let $c_2' = |C_2'|$. By the lower bound on c_2 and (17) we obtain:

$$c_2' \geq c_2 - (n - h - c_2) \geq 3h - \frac{n}{10} - 20\log n - n \geq \frac{13}{40}n - 38\log n \ . \tag{19}$$

Note that each row $i \in C_2'$ has the entry 1 at the index i and the entry -1 at some index $j > h$.

Finally, notice that (18) and (19) imply that $c_1' + c_2' > n/2$ for a sufficiently large value of n. However, as the rows of $M_{\mathcal{A}}$ and $M_{\mathcal{B}}$ are orthogonal, the non-zero entries of each pair of rows $i \in C_1'$ and $j \in C_2'$ must be in pairwise disjoint columns. In particular, we obtain that $2c_1' + 2c_2' \leq n$, yielding a contradiction. Thus, either $\mathcal{A}$ or $\mathcal{B}$ does not meet the requirements of Lemma 3.2, and we deduce that (13) holds. ■

4 Proof of Theorem 1.1 and two lemmas

Let $\mathcal{A}$ and $\mathcal{B}$ denote an ℓ-cross-intersection pair of families in $2^{[n]}$. Recall that in the proof of Theorem 3.1, we argued that if, for instance, $\mathcal{A}$ is not an antichain, then $\bigcup_{B \in \mathcal{B}} B \neq [n]$ (see (9)). In such a case, letting $i \in [n]$ be so that $i \notin B$ for all $B \in \mathcal{B}$, it follows that $\mathcal{A} = \mathcal{A}' \cup \{A \cup \{i\} : A \in \mathcal{A}'\}$ and $\mathcal{B} = \mathcal{B}'$, where $(\mathcal{A}', \mathcal{B}')$ is an optimal ℓ-cross-intersecting pair on $[n] \setminus \{i\}$. Therefore, by induction, the structure of $\mathcal{A}, \mathcal{B}$ is as specified in Theorem 1.1, where the parameter n' (determining the set X in (5)) accounts for the modification of $(\mathcal{A}', \mathcal{B}')$ to $(\mathcal{A}, \mathcal{B})$. The same consideration applies when $\bigcup_{A \in \mathcal{A}} A \neq [n]$, which follows when $\mathcal{B}$ is not an antichain (in this case, the set Y in (5) treats the modification of $\mathcal{B}'$ to $\mathcal{B}$). Altogether, we may assume that $\mathcal{A}, \mathcal{B}$ are both antichains, and furthermore:

$$\bigcup_{A \in \mathcal{A}} A = \bigcup_{B \in \mathcal{B}} B = [n] \ . \tag{20}$$

It remains to prove that in this case $|\mathcal{A}||\mathcal{B}| \leq \binom{2\ell}{\ell} 2^{n-2\ell}$, and that equality holds iff for some

$$\begin{aligned} &\kappa \in \{2\ell - 1, 2\ell\} \ , \ \tau \in \{0, \ldots, \kappa\} \ , \\ &\kappa + \tau = n, \end{aligned} \tag{21}$$

the following holds up to a relabeling of the elements of $[n]$ and swapping $\mathcal{A}, \mathcal{B}$:

$$\begin{aligned} \mathcal{A} &= \left\{ \bigcup_{T \in J} T \ : \ J \subset \left\{ \begin{array}{c} \{1, \kappa+1\}, \ldots, \{\tau, \kappa+\tau\}, \\ \{\tau+1\}, \ldots, \{\kappa\} \end{array} \right\} \ , \ |J| = \ell \right\} , \\ \mathcal{B} &= \left\{ L \cup \{\tau+1, \ldots, \kappa\} : \begin{array}{l} L \subset \{1, \ldots, \tau, \kappa+1, \ldots, \kappa+\tau\} \\ |L \cap \{i, \kappa+i\}| = 1 \text{ for all } i \in [\tau] \end{array} \right\} . \end{aligned} \tag{22}$$

Following the notations of Theorem 3.1, define $\mathcal{F}_{\mathcal{A}}, \mathcal{F}'_{\mathcal{B}}, k, h$ as in (10) and (11), obtaining $k \geq h$. Recall that the proof of Theorem 3.1 implies that $|\mathcal{A}||\mathcal{B}| \leq 2^{k+h+3}/\sqrt{n}$ provided that ℓ is sufficiently large (equation (13)). This implies that if $k + h \leq n - 4$ then:

$$|\mathcal{A}||\mathcal{B}| \leq \frac{1}{2} \cdot \frac{2^n}{\sqrt{n}} \ ,$$

and as $\frac{1}{2} < 1/\sqrt{\pi}$, the pair $\mathcal{A}, \mathcal{B}$ is suboptimal. Assume therefore that $k + h \geq n - 3$:

$$\left\{ \begin{array}{ccc} \frac{n-3}{2} \leq & k & \\ n-3 \leq & k+h & \leq n \end{array} \right. . \tag{23}$$

Observe that, as the rows of $M_{\mathcal{A}}$ are orthogonal to the rows of $M_{\mathcal{B}}$, we may assume without loss of generality that:

$$M_{\mathcal{A}} = \left(\begin{array}{c|c} I_k & * \end{array} \right) \ , \ M_{\mathcal{B}} = \left(\begin{array}{c|c} * & I_h \end{array} \right) \ .$$

To see this, first perform Gauss elimination on a basis for $\mathcal{F}_{\mathcal{A}}$ to obtain $M_{\mathcal{A}}$. Next, perform Gauss elimination on a basis for $\mathcal{F}'_{\mathcal{B}}$, and notice that, as the rows of $M_{\mathcal{A}}$ and $M_{\mathcal{B}}$ are pairwise orthogonal, it is always possible to find a leading non-zero entry at some index $j > k$. Once $M_{\mathcal{B}}$ is in row-reduced echelon form, we may relabel the elements $k+1, \ldots, n$ to obtain the above structure.

We again apply the arguments of Lemma 3.2 on $\mathcal{A}, M_{\mathcal{A}}$ and on $\mathcal{B}, M_{\mathcal{B}}$, only this time we perform the calculations more carefully. Let $R_A \subset [k]$ denote the subset of the rows of $M_{\mathcal{A}}$ which are selected by the process described in Claim 3.3. That is, we repeatedly select an arbitrary column with at least 2 non-zero entries, while one exists, add the rows where it is non-zero to R_A, and delete them from $M_{\mathcal{A}}$. While in Claim 3.3 we repeatedly selected a column with a maximal number of non-zero entries, here we allow an arbitrary choice when selecting the next column with at least 2 non-zero entries. Let $r_A = |R_A|$, and define $R_B \subset [h]$ and $r_B = |R_B|$ similarly for $M_{\mathcal{B}}$.

Let $S_A \subset [k] \setminus R_A$ denote the indices of rows of $M_{\mathcal{A}}$, which belong neither to R_A nor to $\{0, \pm 1\}^n \setminus \{0, 1\}^n$. That is, S_A denotes the rows which were treated by Claim 3.4. Let $s_A = |S_A|$, and define $S_B \subset [h] \setminus R_B$ and $s_B = |S_B|$ similarly for $M_{\mathcal{B}}$.

The following lemma, proved in Section 5, determines the optimal pairs $\mathcal{A}, \mathcal{B}$ when $r_A + s_A = o(n)$:

Lemma 4.1. *If there exists some order of column selection when producing the set R_A such that $r_A + s_A = o(n)$, then $|\mathcal{A}||\mathcal{B}| \leq \binom{2\ell}{\ell} 2^{n-2\ell}$. Furthermore, equality holds iff either:*

$$M_{\mathcal{A}} = \left(\begin{array}{c|c|c||c} & 0 & & 0 \\ I_{k-1} & \vdots & -I_{k-1} & \vdots \\ & 0 & & 0 \\ \hline 0 & 1 & 1\dots1 & 1 \end{array}\right) \ , \ M_{\mathcal{B}} = \left(\begin{array}{c|c|c||c} & -1 & & 0 \\ I_{k-1} & \vdots & I_{k-1} & \vdots \\ & -1 & & 0 \\ \hline\hline 0 & -1 & 0\dots0 & 1 \end{array}\right) \tag{24}$$

$$h \in \{2\ell-2, 2\ell-1\} \ , \ h+k=n \ , \ k \in \{\tfrac{n}{2}, \tfrac{n+1}{2}\} \ , \ B_1 = \cup_{i\in[\ell]}\{(i,k+i)\}$$

or :

$$M_{\mathcal{A}} = \left(\begin{array}{c|c|c|c||c|c} & 0 & 0 & & 0 & 0 \\ I_{k-2} & \vdots & \vdots & -I_{k-2} & \vdots & \vdots \\ & 0 & 0 & & 0 & 0 \\ \hline 0 & 1 & 0 & 1\dots1 & 1 & 1 \\ 0 & 0 & 1 & 1\dots1 & 1 & 1 \end{array}\right) , M_{\mathcal{B}} = \left(\begin{array}{c|c|c|c||c|c} & -1 & -1 & & 0 & 0 \\ I_{k-2} & \vdots & \vdots & I_{k-2} & \vdots & \vdots \\ & -1 & -1 & & 0 & 0 \\ \hline\hline 0 & -1 & -1 & 0\dots0 & 1 & 0 \\ 0 & -1 & -1 & 0\dots0 & 0 & 1 \end{array}\right)$$

$$h \in \{2\ell-2, 2\ell-1\} \ , \ h+k=n \ , \ k \in \{\tfrac{n}{2}, \tfrac{n+1}{2}, \tfrac{n}{2}+1\} \ , \ B_1 = \cup_{i\in[\ell]}\{(i,k+i)\} \tag{25}$$

up to a relabeling of the elements of $[n]$ and the choice of B_1. In both cases above, the pair $(\mathcal{A},\mathcal{B})$ belongs to the family (22) *with $\kappa = h+1$, $\tau = k-1$ and swapping $\mathcal{A},\mathcal{B}$.*

In the above figures (24) and (25), the columns to the right of the double-line-separators and the rows below the double-line-separators appear or not, depending on the value of k.

The remaining case is treated by the next lemma, which is proved in Section 6, and concludes the proof of the theorem:

Lemma 4.2. *If every order of column selection when producing the set R_A gives $r_A + s_A = \Omega(n)$, then $|\mathcal{A}||\mathcal{B}| \leq \binom{2\ell}{\ell} 2^{n-2\ell}$. Furthermore, equality holds iff:*

$$M_{\mathcal{A}} = \left(\begin{array}{c|c|c} I_h & 0 & I_h \\ \hline 0 & I_{k-h} & 0 \end{array}\right) \ , \ M_{\mathcal{B}} = \left(\begin{array}{c|c|c} -I_h & 0 & I_h \end{array}\right) \tag{26}$$

$$k \in \{2\ell-1, 2\ell\} \ , \ h+k=n \ , \ B_1 = [k]$$

up to a relabeling of the elements of $[n]$. In this case, the pair $(\mathcal{A},\mathcal{B})$ belongs to the family (22) *with $\kappa = k$ and $\tau = h$.*

Remark 4.3: It is, in fact, not difficult to check that if, in one order of column selection we have $r_A + s_A = \Omega(n)$, so is the case in any order, but the above formulation suffices for our purpose.

5 Proof of Lemma 4.1

Let $C_1 = [k] \setminus (R_A \cup S_A)$. By the assumption on r_A, s_A and the fact that $k \geq \frac{n-3}{2}$ we deduce that $|C_1| = (1-o(1))k$. Recall that each column of $M_{\mathcal{A}}$ contains at most one non-zero entry in the rows

of C_1, and that each row of C_1 belongs to $\{0,\pm 1\}^n \setminus \{0,1\}^n$. Hence, $n \geq k + |C_1| = (2 - o(1))k$. Altogether, we obtain that:

$$k = \left(\frac{1}{2} + o(1)\right) n \quad , \quad h = \left(\frac{1}{2} - o(1)\right) n \ . \tag{27}$$

The $\{1,-1\}$ entries in each row of C_1 account for $2|C_1| = (1-o(1))n$ distinct columns, leaving at most $o(n)$ columns which may contribute additional values to rows of C_1. Again, as each column contains at most 1 non-zero entry in the rows of C_1, the set of all rows with non-zero entries either in these columns, or in columns $\{k+1,\ldots,n-h\}$ (at most 3 columns), is of size $o(n)$. We obtain that, without loss of generality:

$$M_{\mathcal{A}} = \begin{array}{c} \overset{\leftarrow\cdots\ k\ \cdots\rightarrow}{\overset{\|\leftarrow\leq 3\rightarrow\|}{\overset{\leftarrow\cdots h\cdots\rightarrow}{}}} \\ \left(\begin{array}{c|c|c|c|c} I_{k'} & 0 & 0 & -I_{k'} & 0 \\ 0 & I_{k-k'} & * & * & * \end{array}\right) \end{array} \ , \tag{28}$$

where $k' = (1-o(1))k = (1-o(1))h$. The above structure of $M_{\mathcal{A}}$ provides a quick bound on $|\mathcal{A}|$. Consider column $n-h+1$; if this column contains at least 2 non-zero entries, then we gain a factor of $\frac{3}{4}$ by (14). Otherwise, the fact that $M_{n-h+1,1} = -1$ implies that the coefficient of row 1 is necessarily 0, giving a factor of $\frac{1}{2}$. Therefore:

$$|\mathcal{A}| \leq \frac{3}{4} \cdot 2^k \ . \tag{29}$$

For another corollary of (28), notice that for all $i \in [k']$, row i of $M_{\mathcal{A}}$ contains $1,-1$ in columns $i, n-h+i$ respectively (and 0 in the remaining columns), and is orthogonal to all rows of $M_{\mathcal{B}}$. It follows that columns $i, n-h+i$ are equal in $M_{\mathcal{B}}$ for all $i \in [k']$, and hence:

$$M_{\mathcal{B}} = \begin{array}{c} \overset{\leftarrow\cdots k\cdots\rightarrow}{\overset{\|\leftarrow\leq 3\rightarrow\|}{\overset{\leftarrow\cdots\ h\ \cdots\rightarrow}{}}} \\ \left(\begin{array}{c|c|c|c|c} I_{k'} & * & * & I_{k'} & 0 \\ 0 & * & * & 0 & I_{h-k'} \end{array}\right) \end{array} \ . \tag{30}$$

We claim that the above structure of $M_{\mathcal{B}}$ implies that $r_B + s_B = (1-o(1))h$. Indeed, once we delete the rows $R_B \cup S_B$ from $M_{\mathcal{B}}$, each row must contain an entry of -1, which must reside in one of the columns $k'+1,\ldots,n-h$. As each column contains at most one non-zero entry in rows $[h] \setminus (R_B \cup S_B)$, we deduce that $n-h-k' \geq h - r_B - s_B$, and equivalently:

$$r_B + s_B \geq 2h + k' - n = (1-o(1))h = \left(\frac{1}{2} - o(1)\right) n \ ,$$

where the last two equalities are by (27) and the fact that $k' = (1-o(1))k$. Recall that the analysis of Claim 3.3 implies that, if R_B is nonempty, then at most $2^{r_B} \cdot \min\{1/\sqrt{n}\ ,\ 2/\sqrt{\frac{\pi}{2}(r_B - 2\log n)}\}$ linear combinations of the rows of R_B are valid in order to produce a $\{0,1\}^n$ vector from the rows of $M_{\mathcal{B}}$. Furthermore, if S_B is nonempty, then for each choice of coefficients for the rows $[h] \setminus S_B$, Claim 3.4 implies that at most $2^{s_B}/\sqrt{\frac{\pi}{2}s_B}$ combinations of the rows of S_B are valid in order to produce

a $\{0,1\}^n$ antichain of vectors from the rows of $M_{\mathcal{B}}$. Since in our case we have $r_B + s_B = \Omega(n)$, at least one of r_B, s_B is $\Omega(n)$, and we deduce that:

$$|\mathcal{B}| = O(2^h/\sqrt{n}) \ . \tag{31}$$

Furthermore, if both $r_B = \omega(1)$ and $s_B = \omega(1)$ we get $|\mathcal{B}| = O(\frac{2^h}{\sqrt{r_B s_B}}) = o(2^h/\sqrt{n})$ and hence (regardless of the structure of $M_{\mathcal{A}}$) $|\mathcal{A}||\mathcal{B}| = o(2^{k+h}/\sqrt{n}) \leq o(2^n/\sqrt{\ell})$, showing this cannot be an optimal configuration, as required. The same consequence is obtained if either $r_A = \omega(1)$ or $s_A = \omega(1)$, as in this case $|\mathcal{A}| = o(2^k)$. Assume therefore that $r_A + s_A = O(1)$, and by the above arguments we obtain that:

$$k = \tfrac{n}{2} + O(1) \ , \ h = \tfrac{n}{2} - O(1) \ , \tag{32}$$

$$k' = k - O(1) \ , \tag{33}$$

$$r_B = O(1) \ , \ s_B = h - O(1) \quad \text{or} \quad r_B = h - O(1) \ , \ s_B = O(1) \ . \tag{34}$$

At this point, we claim that either $n = (4 + o(1))\ell$, or the pair $\mathcal{A}, \mathcal{B}$ is suboptimal:

Claim 5.1. *Let $\mathcal{A}, \mathcal{B}$ be as above, then either $|\mathcal{A}||\mathcal{B}| = o(2^n/\sqrt{n})$ or $n = (4 + o(1))\ell$.*

Proof. Fix a choice of coefficients for the last $k - k'$ rows of $M_{\mathcal{A}}$, yielding a linear combination w_A. By the structure of $M_{\mathcal{A}}$ specified in (28), $w_A^{(i)} = 0$ for all $i \in [k']$. Furthermore, if for some index $i \in [k']$, w_A does not equal 1 at index $n - h + i$, then the i-th row of $M_{\mathcal{A}}$ has at most one valid coefficient. Thus, if there are $\omega(1)$ such indices, we deduce that there are at most $o(2^{k'})$ combinations of the rows $[k']$ of $M_{\mathcal{A}}$ which extend w_A to an element of $\mathcal{A}$. Therefore, by (31), this choice of w_A counts for at most $o(2^{k'+h}/\sqrt{n})$ pairs $(A, B) \in \mathcal{A} \times \mathcal{B}$. Summing over all $2^{k-k'}$ choices for w_A, this amounts to at most $o(2^n/\sqrt{n})$ pairs $(A, B) \in \mathcal{A} \times \mathcal{B}$, and we may thus assume that any w_A with non-negligible contribution to $\mathcal{A} \times \mathcal{B}$ has at least $k' - O(1)$ of the indices $j \in [k']$ with

$$w_A^{(j)} = 0 \ , \ w_A^{(n-h+j)} = 1 \ . \tag{35}$$

Next, fix a choice of coefficients for the last $h - k'$ rows of $M_{\mathcal{B}}$, yielding an affine combination (together with χ_{B_1}) w_B, and consider the structure of $M_{\mathcal{B}}$ specified in (30). Every index $j \in [k']$ for which $\chi_{B_1}^{(j)} \neq \chi_{B_1}^{(n-h+j)}$ implies that the row j has at most one valid coefficient. Thus, if there are $\omega(1)$ such indices, it follows that w_B can be extended to at most $o(2^h/\sqrt{n})$ elements of $\mathcal{B}$. To see this, take $m = \omega(1)$ and yet $m = o(n)$ such rows, arbitrarily; there is at most one legal combination for these rows. As $r_B + s_B = \Omega(n)$, the remaining rows have at most $O(2^{h-m}/\sqrt{n})$ combinations, and the result follows.

Altogether, we may assume that $k' - O(1)$ of the indices $j \in [k']$ satisfy:

$$\chi_{B_1}^{(j)} = \chi_{B_1}^{(n-h+j)} \ . \tag{36}$$

Let $L \subset [k']$ denote the indices of $[k']$ which satisfy both (35) and (36). It follows that $|L| = h - O(1)$, and for each $i \in L$, the choice of a coefficient for row i exclusively determines between the cases $i, n + h - i \in B$ and $i, n + h - i \notin B$.

Fix a choice of coefficients for the remaining rows of $M_{\mathcal{A}}$, let $A \in \mathcal{A}$ denote the resulting set, and fix a choice of coefficients for all rows of $M_{\mathcal{B}}$ except those whose indices are in L. For each $i \in L$, let X_i denote the variable whose value is 1 if we choose a coefficient for the row i such that $i, n+h-i \in B$ and 0 otherwise. Recall that A contains precisely one element from each pair $\{i, n+h-i \ : \ i \in L\}$. Therefore, any legal choice of coefficients of the rows L in $M_{\mathcal{B}}$ gives a set B which satisfies:

$$\ell = |A \cap B| = (\sum_{i \in L} X_i) + O(1) \ , \tag{37}$$

where the $O(1)$-term accounts for the intersection of A with at most $n - 2|L| = O(1)$ indices. Choose one of each pair of coefficients for each row of L uniformly at random and independently of the other rows, to obtain that $X = \sum_{i \in L} X_i$ has a binomial distribution $\mathrm{Bin}(\frac{n}{2} - O(1), \frac{1}{2})$. Fix some small $\varepsilon > 0$; by the Chernoff bound (see, e.g., [2], Chapter A.1):

$$\Pr[|X - \frac{n}{4}| > \varepsilon n] \leq O\left(\exp(-\Omega(n))\right) \ ,$$

thus if $|\ell - \frac{n}{4}| > \varepsilon n$ then at most $O(2^h/\exp(\Omega(n)))$ sets $B \in \mathcal{B}$ can be produced from w_B and we are done. We conclude that $\ell = (\frac{1}{4} + o(1))n$. ■

The last claim, along with (34), implies that the case $s_B = h - O(1)$ is suboptimal. Indeed, in this case:

$$|\mathcal{B}| \leq \frac{2^h}{\sqrt{\pi s_B/2}} = (1+o(1))\frac{2^h}{\sqrt{\pi h/2}} = (1+o(1))\frac{2^h}{\sqrt{\pi n/4}} = (1+o(1))\frac{2^h}{\sqrt{\pi \ell}} \ ,$$

where the last inequality is by Claim 5.1. Combining this with (29), we deduce that $|\mathcal{A}||\mathcal{B}|$ is at most $(\frac{3}{4} + o(1))2^n/\sqrt{\pi\ell}$, and that the pair $\mathcal{A}, \mathcal{B}$ is suboptimal.

It remains to deal with the case $r_B = h - O(1)$, in which case we have:

$$|\mathcal{B}| \leq \frac{2^{h+1}}{\sqrt{\pi r_B/2}} = (2+o(1))\frac{2^h}{\sqrt{\pi \ell}} \ , \tag{38}$$

and hence ($|\mathcal{A}| \leq \frac{3}{4} \cdot 2^k$), $|\mathcal{A}||\mathcal{B}| \leq (\frac{3}{2} + o(1))2^{k+h}/\sqrt{\pi\ell}$. If $k + h < n$, it follows that $|\mathcal{A}||\mathcal{B}|$ is at most $(\frac{3}{4} + o(1))2^n/\sqrt{\pi\ell}$, and again the pair $\mathcal{A}, \mathcal{B}$ is suboptimal. We may thus assume:

$$k + h = n \ , \ r_B = h - O(1) \ , \ s_B = O(1) \ .$$

To complete the proof of the lemma, we show that either $|\mathcal{A}||\mathcal{B}| \leq (\delta + o(1))2^n/\sqrt{\pi\ell}$ for some fixed $\delta < 1$, or all columns of $M_{\mathcal{B}}$ except either 1 or 2 have at most 1 non-zero entry, whereas the remaining columns are of the form $(-1, \ldots, -1)$. This will imply that either (24) holds or (25) holds. For this purpose, we must first concentrate on the $(k - k') \times k'$ sub-matrix of $M_{\mathcal{A}}$, on rows $\{k'+1, \ldots, k\}$ and columns $\{k+1, \ldots, k+k'\}$. This sub-matrix appears boxed in diagram (39),

which reflects the form of $M_{\mathcal{A}}$ and $M_{\mathcal{B}}$ given the fact $k+h=n$:

$$M_{\mathcal{A}} = \left(\begin{array}{c|c|c|c} I_{k'} & 0 & -I_{k'} & 0 \\ 0 & I_{k-k'} & \boxed{*} & * \end{array}\right) \quad . \qquad (39)$$

$$M_{\mathcal{B}} = \left(\begin{array}{c|c|c|c} I_{k'} & * & I_{k'} & 0 \\ 0 & * & 0 & I_{h-k'} \end{array}\right)$$

Suppose the linear combination of rows $k'+1,\ldots,k$ of $M_{\mathcal{A}}$ is some vector w_A. A key observation is the following: if w_A has $\omega(1)$ entries not equal to 1 in indices $\{k+1,\ldots,k+k'\}$, then at most $o(2^{k'})$ combinations of the remaining rows can be added to w_A to produce a vector in $\{0,1\}^n$. This follows directly from the structure of $M_{\mathcal{A}}$ in (39), as the fact that $w_A^{(k+j)} \neq 1$ forces the coefficient of row j to be 0. Using the above observation, we will show that either $|\mathcal{A}| \leq (\frac{3}{8}+o(1))2^k$, or at most $O(1)$ columns of $M_{\mathcal{A}}$ with indices $\{k+1,\ldots,k+k'\}$ are not of one of the forms $\{(-1,1,0,\ldots,0),(-1,1,1,0,\ldots,0)\}$ (at some coordinate order). Consider the following three cases:

(I) $\omega(1)$ **columns of $M_{\mathcal{A}}$ contain at least 3 non-zero entries in rows $\{k'+1,\ldots,k\}$:** Let S denote the indices of columns in $\{k+1,\ldots,k+k'\}$ for which $M_{\mathcal{A}}$ has non-zero entries in rows $\{k'+1,\ldots,k\}$. The Littlewood-Offord Lemma implies that, whenever there are t non-zero entries in a single column in these rows, then at most $m = 2^{k-k'-t}\binom{t}{\lfloor t/2 \rfloor}$ of the $2^{k-k'}$ possible linear combinations of these rows can produce a value of 1. Notice that for $t \geq 3$ we get $\binom{t}{\lfloor t/2 \rfloor}/2^t \leq \frac{3}{8}$, hence $m/2^{k-k'} \leq \frac{3}{8}$. Next, let each column which has at least 3 non-zero entries in rows $\{k'+1,\ldots,k\}$ "rate" m linear combinations, including all those for which it gives a value of 1. It follows that choosing any combination for rows $\{k'+1,\ldots,k\}$ excluding the most popular set of m linear combinations, yields values not equal to 1 in at least $|S|/\binom{2^{k-k'}}{m} = \Omega(|S|) = \omega(1)$ columns, hence (by the above observation) such combinations contribute $o(2^k)$ vectors to $\mathcal{A}$. We deduce that $|\mathcal{A}| \leq (\frac{3}{8}+o(1))2^k$.

(II) $\omega(1)$ **columns of $M_{\mathcal{A}}$ contain 2 non-zero entries $\neq (1,1)$ in rows $\{k'+1,\ldots,k\}$:** The argument here is similar to the argument in the previous item. If a column has two non-zero entries $(x,y) \neq (1,1)$ in rows $k'+1,\ldots,k$, then the possible values of the linear combination at this column are $\{0,x,y,x+y\}$. At most 1 of these 4 values can be 1, hence at most $m = 2^{k-k'-2}$ of the combinations yield a value of 1 at this column. By the above argument, we deduce that $|\mathcal{A}| \leq (\frac{1}{4}+o(1))2^k$.

(III) $\omega(1)$ **columns of $M_{\mathcal{A}}$ contain at most 1 non-zero entry $\neq 1$ in rows $\{k'+1,\ldots,k\}$:** this case is the simplest, following directly from the observation. Indeed, every linear combination of the rows $k'+1,\ldots,k$ has $\omega(1)$ entries which do not equal 1 in columns $\{k+1,\ldots,k+k'\}$, hence $|\mathcal{A}| = o(2^k)$.

Note that if $|\mathcal{A}| \leq (\frac{3}{8}+o(1))2^k$, then $|\mathcal{A}||\mathcal{B}| \leq (\frac{3}{4}+o(1))2^n/\sqrt{\pi\ell}$ by (38), as required. Assume therefore that $M_{\mathcal{A}}$ has at most $O(1)$ columns among $\{k+1,\ldots,k+k'\}$, whose set of non-zero

entries in rows $\{k'+1,\ldots,k\}$ is neither $\{1\}$ nor $\{1,1\}$. We use the abbreviation $\{1\}$-columns and $\{1,1\}$-columns for the $k'-O(1)$ remaining columns whose non-zero entries in rows $\{k'+1,\ldots,k\}$ of $M_{\mathcal{A}}$ are $\{1\}$ and $\{1,1\}$ respectively; according to this formulation:

$$k'-O(1) \text{ of columns } \{k+1,\ldots,k'\} \text{ of } M_{\mathcal{A}} \text{ are } \{1\}\text{-columns or } \{1,1\}\text{-columns .} \tag{40}$$

The two cases of whether there are $\omega(1)$ or $O(1)$ $\{1\}$-columns, are treated by Claims 5.2 and 5.3 respectively, and determine which of the two optimal families, stated in (24),(25), is obtained. These two claims are stated and proved in Subsections 5.1 and 5.2.

5.1 The optimal family (24)

Claim 5.2. *If $\omega(1)$ of columns $\{k+1,\ldots,k+k'\}$ of $M_{\mathcal{A}}$ are $\{1\}$-columns, then (24) holds.*

Proof. It follows that some row of $\{k'+1,\ldots,k\}$ contains a value of 1, which is the single non-zero entry of this column in these rows, in $\omega(1)$ columns of $\{k+1,\ldots,k+k'\}$ (take the most popular row of $\{k'+1,\ldots,k\}$). Without loss of generality, assume that this row is row k, the last row of $M_{\mathcal{A}}$. By the observation above, the coefficient for row k of $M_{\mathcal{A}}$ must be 1, otherwise only $o(2^k)$ combinations of the remaining rows produce vectors in $\{0,1\}^n$. This has several consequences:

(1) Row k contains the value 1 in columns $\{k+1,\ldots,k+k'\}$. To see this, suppose $(M_{\mathcal{A}})_{k,k+j}\neq 1$ for some $j\in[k']$. If $k'>k-2$, that is, there are no non-zero values in column j except for those in rows j and k (see (39)), then $|\mathcal{A}|\leq\left(\frac{1}{4}+o(1)\right)2^k$: the coefficient 0 for row k contributes $o(2^k)$ vectors to $|\mathcal{A}|$, whereas the coefficient 1 for that row forces the choice of 0 as the coefficient for row j. Otherwise, in the case $k\geq k'+2$, we have $|\mathcal{A}|\leq\left(\frac{\delta}{2}+o(1)\right)2^k$, where $\delta=1-2^{-(k-k'-1)}<1$, since the 0 coefficient for row k again contributes $o(2^k)$ vectors to $|\mathcal{A}|$, and the coefficient 1 for row k prohibits the choice of 1 for row j and 0 for rows $k'+1,\ldots,k-1$.

(2) Row k contains $\{0,1\}$ values in columns $\{k+k'+1,\ldots,n\}$. Indeed, if $(M_{\mathcal{A}})_{k,k+j}\notin\{0,1\}$ for some $j\in\{k'+1,\ldots,n-k\}$, then the all-zero choice of coefficients for rows $\{k'+1,\ldots,k-1\}$ becomes illegal when giving row k the coefficient 1, implying that $|\mathcal{A}|\leq\left(\frac{\delta}{2}+o(1)\right)2^k$, where $\delta=1-2^{-(k-k'-1)}$. Of course, $\delta<1$, since whenever $k\leq k'-1$ all entries above $(M_{\mathcal{A}})_{k,k+j}$ are 0, hence any combination that gives row k the coefficient 1 becomes illegal (yielding just $o(2^k)$ vectors in $\mathcal{A}$).

(3) If $M'_{\mathcal{A}}$ is the $(k-1)\times n$ sub-matrix of rows $\{1,\ldots,k-1\}$ of $M_{\mathcal{A}}$ (that is, the matrix obtained by erasing the last row of $M_{\mathcal{A}}$), then every column of $M'_{\mathcal{A}}$ contains at most 1 non-zero entry, and every row of $M'_{\mathcal{A}}$ belongs to $\{0,\pm1\}^n\setminus\{0,1\}^n$. To see this, notice that the coefficient of row k is set to 1, otherwise we obtain at most $o(2^k)$ vectors. We can thus regard this row as an affine vector in $\{0,1\}^n$, and consider the 2^{k-1} combinations for the remaining rows. Now, a column of $M'_{\mathcal{A}}$ with at least 2 non-zero entries implies that the number of such legal combinations (resulting in a vector in $\{0,1\}^n$) is at most $\frac{3}{4}\cdot 2^{k-1}$, and a row which does not

belong to $\{0,\pm 1\}^n \setminus \{0,1\}^n$ implies that this number is at most 2^{k-2}. In both cases, we get $|\mathcal{A}| \leq (\frac{3}{8} + o(1))2^k$.

(4) Every row of $M'_{\mathcal{A}}$ has at most 2 non-zero values: assume that the converse holds, that is, that row $m \in [k-1]$ contains at least 2 non-zero entries in indices $\{k+1,\ldots,n\}$. Since each of the $k-1$ rows of $M'_{\mathcal{A}}$ must contain a -1 value in an exclusive column, it leaves at most $n-k-(k-1) = n-2k+1 \leq 1$ column (recall that $k \geq \frac{n}{2}$), which can contribute 1 additional non-zero value to row m. We deduce that row m has precisely two non-zero entries at columns $\{k+1,\ldots,n\}$. However, in this case column m of $M_{\mathcal{B}}$ has precisely two non-zero entries , since (39) and the orthogonality of $M_{\mathcal{A}}, M_{\mathcal{B}}$ imply that:

$$(M_{\mathcal{A}})_{i,k+j} = -(M_{\mathcal{B}})_{j,i} \quad \text{for all } i \in [k] \text{ and } j \in [h] \tag{41}$$

(the inner product of row i of $M_{\mathcal{A}}$ and row j of $M_{\mathcal{B}}$ is $(M_{\mathcal{A}})_{i,k+j} + (M_{\mathcal{B}})_{j,i} = 0$). From the same reason, column k of $M_{\mathcal{B}}$ has at least k' non-zero entries (as row k of $M_{\mathcal{A}}$ has the value 1 in columns $\{k+1,\ldots,k+k'\}$). Therefore, performing the process of Claim 3.3 first on column m and then on column k of $M_{\mathcal{B}}$ gives $|\mathcal{B}| \leq \frac{3}{4} \cdot \frac{2+o(1)}{\sqrt{\pi\ell}}$, hence the pair $\mathcal{A}, \mathcal{B}$ is suboptimal.

Items (3) and (4) imply that, if the pair $\mathcal{A}, \mathcal{B}$ is optimal, then without loss of generality, $M'_{\mathcal{A}}$ is of the form $\left(\begin{smallmatrix} I_{k-1} & | & 0 & | & -I_{k-1} & \| & 0 \\ & & 0 & & & & 0 \end{smallmatrix}\right)$, as each row has $1, -1$ in exclusive columns and 0 everywhere else. In particular, $k' = k-1$, and since $k \geq n/2$ and $k + k' \leq n$, we get:

$$k = h = \frac{n}{2} \quad \text{or} \quad (k = \frac{n+1}{2} \ , \ h = \frac{n-1}{2}) \ , \tag{42}$$

and without loss of generality (using the orthogonality of $M_{\mathcal{A}}, M_{\mathcal{B}}$):

$$M_{\mathcal{A}} = \left(\begin{array}{c|c|c||c} & 0 & & 0 \\ I_{k-1} & \vdots & -I_{k-1} & \vdots \\ & 0 & & 0 \\ \hline 0\ldots0 & 1 & 1\ldots1 & 0/1 \end{array}\right) \ , \ M_{\mathcal{B}} = \left(\begin{array}{c|c|c||c} & -1 & & 0 \\ I_{k-1} & \vdots & I_{k-1} & \vdots \\ & -1 & & 0 \\ \hline\hline 0\ldots0 & 0/-1 & 0\ldots0 & 1 \end{array}\right) \ , \tag{43}$$

where the last column of $M_{\mathcal{A}}$ and the last row and column of $M_{\mathcal{B}}$ do not exist in case $k = (n+1)/2$. If $h = n/2$ and $(M_{\mathcal{B}})_{h,k} = 0$ (as opposed to -1), then $|\mathcal{B}| \leq (1+o(1))2^h/\sqrt{\pi\ell}$: the first $h-1$ rows have at most $(2+o(1))2^{h-1}/\sqrt{\pi\ell}$ combinations by the usual Littlewood-Offord argument on column k, and when adding row h we must form an antichain. It follows that if $k = h = n/2$, then $(M_{\mathcal{B}})_{h,k} = -1$ and, by orthogonality, $(M_{\mathcal{A}})_{k,n} = 1$:

$$M_{\mathcal{A}} = \left(\begin{array}{c|c|c||c} & & & \vdots \\ \ddots & & & 0 \\ \hline 0\ldots0 & 1 & 1\ldots1 & 1 \end{array}\right) \ , \ M_{\mathcal{B}} = \left(\begin{array}{c|c|c||c} & & & \vdots \\ \ddots & & & 0 \\ \hline\hline 0\ldots0 & -1 & 0\ldots0 & 1 \end{array}\right) \ .$$

Finally, notice that the above structure of $M_{\mathcal{A}}$ implies that the coefficient for row k is always 1: a coefficient of 0 necessarily results in the all-zero vector, which is forbidden in $\mathcal{A}$ (for instance, since $\mathcal{A}$ is an antichain, or since $\ell > 0$). Therefore:

$$|\mathcal{A}| \leq 2^{k-1} \ .$$

If $\chi_{B_1}^{(j)} \neq \chi_{B_1}^{(k+j)}$ for some $j \in [k-1]$, we must assign the coefficient 0 to row j of $M_{\mathcal{B}}$, and we are done, as in this case $|\mathcal{B}| \leq (1+o(1))2^h/\sqrt{\pi\ell}$. Assume therefore that $\chi_{B_1}^{(j)} = \chi_{B_1}^{(k+j)}$ for all $j \in [k-1]$, and define:

$$P = \{i \in [h] : k+i \notin B_1\} = \{i \in [h] : \chi_{B_1}^{(k+i)} = 0\} \ , \ Q = [h] \setminus P \ .$$

Every row $i \in P$ of $M_{\mathcal{B}}$ has $\{0,1\}$ as the set of possible coefficients, and every row $i \in Q$ has $\{0,-1\}$ as the possible coefficients. Take $B \in \mathcal{B}$, and suppose that the affine combination which produces B assigns the coefficient 1 to p rows of P ($0 \leq p \leq |P|$), and assigns the coefficient -1 to q rows of Q ($0 \leq q \leq |Q|$). It follows from (43) that for all $A \in \mathcal{A}$:

$$\ell = |A \cap B| = p + (|Q| - q) + \chi_B^{(k)} \ . \tag{44}$$

Let $\mathcal{B}_0$ denote the sets $\{B \in \mathcal{B} : k \notin B\}$, and let $\mathcal{B}_1 = \mathcal{B} \setminus \mathcal{B}_0$. By (44), we obtain that $q = p + |Q| - \ell$ if $k \notin B$, hence:

$$|\mathcal{B}_0| \leq \sum_{p=0}^{|P|} \binom{|P|}{p} \binom{|Q|}{p+|Q|-\ell} = \sum_{p=0}^{|P|} \binom{|P|}{p} \binom{|Q|}{\ell-p} = \binom{h}{\ell} \ .$$

Similarly, if $k \in B$ then $q = p + |Q| - \ell + 1$, and it follows that: $|\mathcal{B}_1| \leq \binom{h}{\ell-1}$. Altogether:

$$|\mathcal{B}| = |\mathcal{B}_0| + |\mathcal{B}_1| \leq \binom{h}{\ell} + \binom{h}{\ell-1} = \binom{h+1}{\ell} \ ,$$

and as $|\mathcal{A}| \leq 2^{k-1}$:

$$|\mathcal{A}||\mathcal{B}| \leq \binom{h+1}{\ell} 2^{n-h-1} \ . \tag{45}$$

As the maxima of the function $f(x) = \binom{x}{\ell} 2^{-x}$ on the domain $\mathbb{N}$ are achieved at $x \in \{2\ell-1, 2\ell\}$, we conclude that $h \in \{2\ell-2, 2\ell-1\}$ (otherwise $|\mathcal{A}||\mathcal{B}| < \binom{2\ell}{\ell} 2^{n-2\ell}$). Finally, recalling that:

$$\chi_B^{(k)} = q - p + \chi_{B_1}^{(k)} \ , \tag{46}$$

and combining (44) and (46) we get:

$$\ell = |Q| + \chi_{B_1}^{(k)} \ .$$

Therefore, whenever $\chi_{B_1}^{(k)} = 0$ we get $|Q| = \ell$, hence $B = \cup_{i \in [\ell]} \{(i, k+i)\}$ for some $B \in \mathcal{B}$. Letting B_1 denote this set B without loss of generality, we obtain the statement of (24).

Finally, let us link the above to the optimal family (22). Define:

$$X = \begin{cases} \{k, n\} & \text{if } k = \frac{n}{2} \\ \{k\} & \text{if } k = \frac{n+1}{2} \end{cases} \ .$$

Each set $A \in \mathcal{A}$ is obtained by choosing one out of each pair of elements $\big\{\{i, k+i\} : i \in [k-1]\big\}$, then adding these $k-1$ chosen elements to the elements of X. Define:

$$Y = \begin{cases} \big\{\{i, k+i\} : i \in [k-1]\big\} \cup \big\{\{n\}\big\} & \text{if } k = \frac{n}{2} \\ \big\{\{i, k+i\} : i \in [k-1]\big\} & \text{if } k = \frac{n+1}{2} \end{cases} \ .$$

Each set $B \in \mathcal{B}_1$ (that is, those sets which contain k) has, in addition to k, $\ell - 1$ objects of Y. Each set $B \in \mathcal{B}_0$ is the union of ℓ objects of Y, and altogether, all sets $B \in \mathcal{B}$ are the union of ℓ objects of $Y \cup \big\{\{k\}\big\}$. As the last set holds the $k-1$ pairs $\{i, k+i\}$ for $i \in [k-1]$ and the single elements corresponding to X, this fits the description of (22) for $\kappa = h+1$, $\tau = k-1$ and swapping $\mathcal{A}, \mathcal{B}$. ■

5.2 The optimal family (25)

Claim 5.3. *If $O(1)$ of columns $\{k+1, \ldots, k+k'\}$ of $M_{\mathcal{A}}$ are $\{1\}$-columns, then (25) holds.*

Proof. By the assumption and by (40), we obtain that $k' - O(1)$ of the columns $\{k+1, \ldots, k+k'\}$ are $\{1,1\}$-columns, that is, there are $k' - O(1)$ columns $j \in \{k+1, \ldots, k+k'\}$ where there are precisely two non-zero entries in rows $\{k'+1, \ldots, k\}$, and both entries are equal to 1. For each such column j, let $i_1(j), i_2(j) \in \{k'+1, \ldots, k\}$ denote the rows where these two entries are located. Assume that, without loss of generality, the pair of rows $k-1, k$ is the most popular pair among the above pairs of rows $\{(i_1(j), i_2(j)) : j \text{ is a } \{1,1\}\text{-column}\}$; it follows that there are $\omega(1)$ columns (and in fact, $\Omega(k')$ columns) $j \in \{k+1, \ldots, k+k'\}$ such that:

$$\begin{cases} (M_{\mathcal{A}})_{k-1,j} = (M_{\mathcal{A}})_{k,j} = 1 \ , \\ (M_{\mathcal{A}})_{i,j} = 0 \text{ for all } i \in \{k'+1, \ldots, k-2\} \ . \end{cases}$$

Hence, if we assign the same coefficient to rows $k-1, k$ then we obtain $\omega(1)$ values which differ from 1 in columns $\{k+1, \ldots, k'\}$, and contribute $o(2^k)$ vectors to $\mathcal{A}$. We must therefore assign the coefficient 1 to precisely one of the rows $k-1, k$ (and assign the coefficient 0 to the other).

The arguments given in the proof of Claim 5.2 regarding row k readily imply the following analogous results on rows $k-1, k$:

(1) Rows $k-1, k$ contain the value 1 in columns $\{k+1, \ldots, k\}$.

(2) Rows $k-1, k$ belong to $\{0,1\}^n$.

(3) If $M'_{\mathcal{A}}$ is the $(k-2) \times n$ sub-matrix of rows $\{1, \ldots, k-2\}$ of $M_{\mathcal{A}}$, then every column of $M'_{\mathcal{A}}$ contains at most 1 non-zero entry, and every row of $M'_{\mathcal{A}}$ belongs to $\{0, \pm 1\}^n \setminus \{0,1\}^n$.

(4) Every row of $M'_{\mathcal{A}}$ contains at most 2 non-zero entries.

By the last two items, we deduce that if $\mathcal{A}, \mathcal{B}$ is an optimal pair, then without loss of generality, $M'_{\mathcal{A}} = \left(\begin{smallmatrix} I_{k-2} | 0 | -I_{k-2} | 0 \end{smallmatrix} \right)$, and in particular, $k' = k-2$. The constraints $k \geq n/2$ and $k + k' \leq n$ now imply:

$$k = h = \frac{n}{2} \quad \text{or} \quad \left(k = \frac{n+1}{2} \ , \ h = \frac{n-1}{2}\right) \quad \text{or} \quad \left(k = \frac{n}{2} + 1 \ , \ h = \frac{n}{2} - 1\right) \ , \tag{47}$$

and by orthogonality:

$$M_{\mathcal{A}} = \left(\begin{array}{c|c|c|c||c|c} & 0 & 0 & & 0 & 0 \\ I_{k-2} & \vdots & \vdots & -I_{k-2} & \vdots & \vdots \\ & 0 & 0 & & 0 & 0 \\ \hline 0 & 1 & 0 & 1\dots1 & 0/1 & 0/1 \\ \hline 0 & 0 & 1 & 1\dots1 & 0/1 & 0/1 \end{array}\right), M_{\mathcal{B}} = \left(\begin{array}{c|c|c|c||c|c} & -1 & -1 & & 0 & 0 \\ I_{k-2} & \vdots & \vdots & I_{k-2} & \vdots & \vdots \\ & -1 & -1 & & 0 & 0 \\ \hline\hline 0 & 0/-1 & 0/-1 & 0\dots0 & 1 & 0 \\ \hline 0 & 0/-1 & 0/-1 & 0\dots0 & 0 & 1 \end{array}\right), \tag{48}$$

where the last two columns of $M_{\mathcal{A}}$ and the last two rows and columns of $M_{\mathcal{B}}$ are optional, depending on whether $k = \frac{n}{2}+1$, $k = \frac{n+1}{2}$ or $k = \frac{n}{2}$ (where we have 0, 1 or 2 of the last columns of $M_{\mathcal{A}}$ and the last rows and columns of $M_{\mathcal{B}}$ respectively).

By (48), it now follows that choosing the same coefficient for both rows $k-1, k$ does not produce sets in $\mathcal{A}$ (so far we only showed that it produces $o(2^k)$ sets in $\mathcal{A}$). Indeed, assigning the coefficient 0 to both these rows can only yield the all-zero vector, forbidden in $\mathcal{A}$ (for instance, as $\ell > 0$). Assigning the coefficient 1 to rows $k-1, k$ can only yield a vector which is 1 in every coordinate $j \in [2k-2]$, and is the sum of the two rows $k-1, k$ in columns $2k-1, 2k$ if these columns exist. Hence, if this vector belongs to $\{0,1\}^n$, then it contains any set which can be produced from $M_{\mathcal{A}}$, and we have $|\mathcal{A}| = 1$, and a suboptimal pair $\mathcal{A}, \mathcal{B}$. It follows that:

$$|\mathcal{A}| \leq 2^{k-1} \ .$$

Our next goal is to show that if row $q \in \{k-1, k\}$ of $M_{\mathcal{B}}$ exists, then its entries in columns $k-1, k$ (marked by $0/-1$ in (48)) are both -1. Let $q \in \{k-1, k\}$ denote a row of $M_{\mathcal{B}}$, let $m \in \{1, 2\}$ denote the number of rows of $\{k-1, k\}$ in $M_{\mathcal{B}}$, and let $q' \neq q$ denote the additional row of $\{k-1, k\}$ in $M_{\mathcal{B}}$ if $m = 2$. Since $m = 1$ iff $k = \frac{n+1}{2}$ and $m = 2$ iff $k = \frac{n}{2}$, it follows that $m = 2 - (k - h)$.

First, assume that $(\mathbf{M}_{\mathcal{A}})_{\mathbf{q},\mathbf{k-1}} = (\mathbf{M}_{\mathcal{A}})_{\mathbf{q},\mathbf{k}} = \mathbf{0}$. It follows that row q is in $\{0,1\}^n$, and since $\mathcal{B}$ is an antichain, we get an additional factor of $\frac{1}{2}$ on $|\mathcal{B}|$ (first apply the Littlewood-Offord Lemma on the remaining rows with respect to column k, then consider the coefficient for row q). It follows that $|\mathcal{B}| \leq (1+o(1))\frac{2^h}{\sqrt{\pi\ell}}$, and that $|\mathcal{A}||\mathcal{B}| \leq (\frac{1}{2}+o(1))2^n/\sqrt{\pi\ell}$.

Second, assume that $(\mathbf{M}_{\mathcal{A}})_{\mathbf{q},\mathbf{k-1}} \neq (\mathbf{M}_{\mathcal{A}})_{\mathbf{q},\mathbf{k}}$. Let t_1 denote the number of sets $B \in \mathcal{B}$ produced from $M_{\mathcal{B}}$ by assigning the coefficient $\alpha \neq 0$ to row q, and the coefficient 0 to row q' (if this row exists), and let $t_2 = |\mathcal{B}| - t_1$. Consider a set B counted by t_1: since row q' does not take part in the affine combinations, the combination of rows $[k-2]$ together with χ_{B_1} sums up to the same value, some λ, in the two columns $k-1, k$ (these two columns are identical in rows $[k-2]$). The fact that indices $k-1, k$ of the resulting vector, χ_B, are $\{\lambda, \lambda-\alpha\}$, forces λ to be equal to α. We can thus apply the Littlewood-Offord Lemma on rows $[k-2]$ (with respect to column k, which has 1 target value), and deduce that:

$$t_1 \leq (1+o(1))\frac{2^{k-2}}{\sqrt{\pi\ell}} \ .$$

To obtain an upper bound on t_2, for each of the remaining 2^m-1 combinations of rows $\{k-1,k\}$ in $M_{\mathcal{B}}$, column k has at most 2 target values (in order to give a $\{0,1\}$ final value), hence, by the Littlewood-Offord Lemma:

$$t_2 \leq (2^m-1)(2+o(1))\frac{2^{k-2}}{\sqrt{\pi\ell}} \ .$$

It follows that:

$$|\mathcal{B}| = t_1+t_2 \leq (2-2^{-m}+o(1))\frac{2^{m+k-2}}{\sqrt{\pi\ell}} = (2-2^{-m}+o(1))\frac{2^h}{\sqrt{\pi\ell}} \ ,$$

where in the last equality we used the fact that $m=2-(k-h)$. The fact that $|\mathcal{A}| \leq 2^{k-1}$ now implies that the pair $\mathcal{A},\mathcal{B}$ is suboptimal.

Having ruled out the cases $(M_{\mathcal{A}})_{q,k-1} = (M_{\mathcal{A}})_{q,k} = 0$ and $(M_{\mathcal{A}})_{q,k-1} \neq (M_{\mathcal{A}})_{q,k}$, we deduce that:

$$(M_{\mathcal{A}})_{q,k-1} = (M_{\mathcal{A}})_{q,k} = -1 \ ,$$

hence the structure of $M_{\mathcal{A}}, M_{\mathcal{B}}$ is:

$$M_{\mathcal{A}} = \left(\begin{array}{cccc||cc} & & \ddots & & \vdots & \vdots \\ & & & & 0 & 0 \\ \hline 0 & 1 & 0 & 1\ldots1 & 1 & 1 \\ \hline 0 & 0 & 1 & 1\ldots1 & 1 & 1 \end{array}\right) \ , \ M_{\mathcal{B}} = \left(\begin{array}{cccc||cc} & & \ddots & & \vdots & \vdots \\ & & & & 0 & 0 \\ \hline\hline 0 & -1 & -1 & 0 & 1 & 0 \\ \hline 0 & -1 & -1 & 0 & 0 & 1 \end{array}\right) \ ,$$

as specified in (25). To conclude the proof of the claim, recall that every $A \in \mathcal{A}$ has precisely one of the elements $k-1,k$, hence the analysis of $|A \cap B|$ for all $B \in \mathcal{B}$ is exactly the same as in Claim 5.2 (precisely one of the columns $k-1,k$ of $M_{\mathcal{B}}$ effects the intersection). It follows that $|\mathcal{A}||\mathcal{B}| \leq \left(\binom{h}{\ell}+\binom{h}{\ell-1}\right)2^{n-h-1} = \binom{h+1}{\ell}2^{n-h-1}$, and hence $h \in \{2\ell-2,2\ell-1\}$, otherwise $\mathcal{A},\mathcal{B}$ is a suboptimal pair. Similarly, the arguments of Claim 5.2 imply that $|Q|=\ell$, where Q is the set of indices $\{i \in [h] : k+i \in B_1\}$, and without loss of generality, we can take B_1 to be $\cup_{i\in[\ell]}\{i,k+i\}$. Altogether, (25) holds.

It remains to link the above to the optimal family (22). Define:

$$X = \begin{cases} \{n-1,n\} & \text{if } k=\frac{n}{2} \\ \{n\} & \text{if } k=\frac{n+1}{2} \\ \emptyset & \text{if } k=\frac{n}{2}+1 \end{cases} \ .$$

Recall that precisely one of the rows $k-1,k$ receives the coefficient 1 in a linear combination which produces some $A \in \mathcal{A}$ from $M_{\mathcal{A}}$. It follows that each set $A \in \mathcal{A}$ is obtained by choosing one out of each pair of elements $\big\{\{i,k+i\} : i \in [k-2]\big\} \cup \big\{\{k-1,k\}\big\}$, then adding these $k-1$ chosen elements to the elements of X. Define:

$$Y = \begin{cases} \big\{\{i,k+i\} : i \in [k-2]\big\} \cup \big\{\{n-1\},\{n\}\big\} & \text{if } k=\frac{n}{2} \\ \big\{\{i,k+i\} : i \in [k-2]\big\} \cup \big\{\{n\}\big\} & \text{if } k=\frac{n+1}{2} \\ \big\{\{i,k+i\} : i \in [k-2]\big\} & \text{if } k=\frac{n}{2}+1 \end{cases} \ .$$

Recall that, for all $B \in \mathcal{B}$, the elements $k-1, k$ are either both in B or both not in B. If $k-1, k \notin B$, then B is the union of ℓ elements of Y. Otherwise, B contains, in addition to $\{k-1, k\}$, the union of $\ell - 1$ elements of Y. Altogether, all sets $B \in \mathcal{B}$ are the union of ℓ objects of $Y \cup \big\{\{k-1, k\}\big\}$. As the last set holds the $k-2$ pairs $\{i, k+i\}$ for $i \in [k-2]$, the pair $\{k-1, k\}$ and the single elements corresponding to X, this fits the description of (22) for $\kappa = h+1$, $\tau = k-1$ and swapping $\mathcal{A}, \mathcal{B}$.

This completes the proof of Claim 5.3 and of Lemma 4.1. ■

6 Proof of Lemma 4.2

The assumption that $r_A + s_A = \Omega(n)$ implies that $|\mathcal{A}| = O(2^k/\sqrt{n})$. Thus, if $r_B + s_B = \omega(1)$ we deduce that $|\mathcal{A}||\mathcal{B}| = o(2^n/\sqrt{n})$ and we are done. Assume therefore that $r_B + s_B = O(1)$, and let $C_2 = [h] \setminus (R_B \cup S_B)$. By definition of R_B and S_B, the following holds:

- Every column of $M_{\mathcal{B}}$ contains at most 1 non-zero value in the rows of C_2.
- Every row of C_2 belongs to $\{0, \pm 1\}^n \setminus \{0, 1\}^n$.

We wish to show that $M_{\mathcal{B}}$ is roughly of the form $(-I_h \mid 0 \mid I_h)$, although so far we did not obtain any restriction on the number of rows in C_2 with more than 2 non-zero entries in $M_{\mathcal{B}}$. In contrast to the analysis of $M_{\mathcal{A}}$ in Lemma 4.1, this does not follow directly from the fact that $r_B + s_B = O(1)$, as h might be substantially smaller than $n/2$ (as opposed to k).

We therefore return to $M_{\mathcal{A}}$ and claim that at most $O(1)$ columns of $M_{\mathcal{A}}$ contain at least 2 non-zero entries in a **cascading** manner. In other words, the process where we repeatedly select an arbitrary column of $M_{\mathcal{A}}$ with at least two non-zero entries, and remove the rows where it is non-zero from the matrix, ends after at most $O(1)$ steps. To see this, assume that $t = \omega(1)$ such columns exist: $j_1, \ldots, j_t$. Perform the process of creating R_A, beginning with these columns in this precise order: choose column j_i at step i for $i \in [t]$. By the assumption of the lemma, $r_A + s_A = \Omega(n)$, hence two cases are possible:

- $r_A = o(n)$: in this case $s_A = \Omega(n)$. Clearly, $r_A \geq 2t = \omega(1)$ by the assumption, and the additional $O(1/\sqrt{n})$ factor resulting from the rows S_A implies that $|\mathcal{A}| = o(2^k/\sqrt{n})$.
- $r_A = \Omega(n)$: by definition, $r_A = \sum_{i=1}^{t} r_i$. If for some $i, j \leq t$ we have $r_i, r_j = \omega(\sqrt{n})$ then $|\mathcal{A}| = o(2^k/\sqrt{n})$. Recall that if $t \geq 4 \log n$, then $|\mathcal{A}| \leq 2^k(\frac{3}{4})^t \leq 2^k/n$. These two facts imply that precisely one i satisfies $r_i = \Omega(n)$. Therefore, column i gives a factor of $O(1/\sqrt{n})$, and the remaining $t-1$ columns give a factor of $o(1)$ as $t = \omega(1)$ and each such column contributes a factor of at most $\frac{3}{4}$. Altogether, we deduce that $|\mathcal{A}| = o(2^k/\sqrt{n})$.

Assume therefore that $M_{\mathcal{A}}$ contains at most $O(1)$ columns which contain at least 2 non-zero entries in a cascading manner. As we next show, returning to $M_{\mathcal{B}}$, this implies that at most $O(1)$ rows of

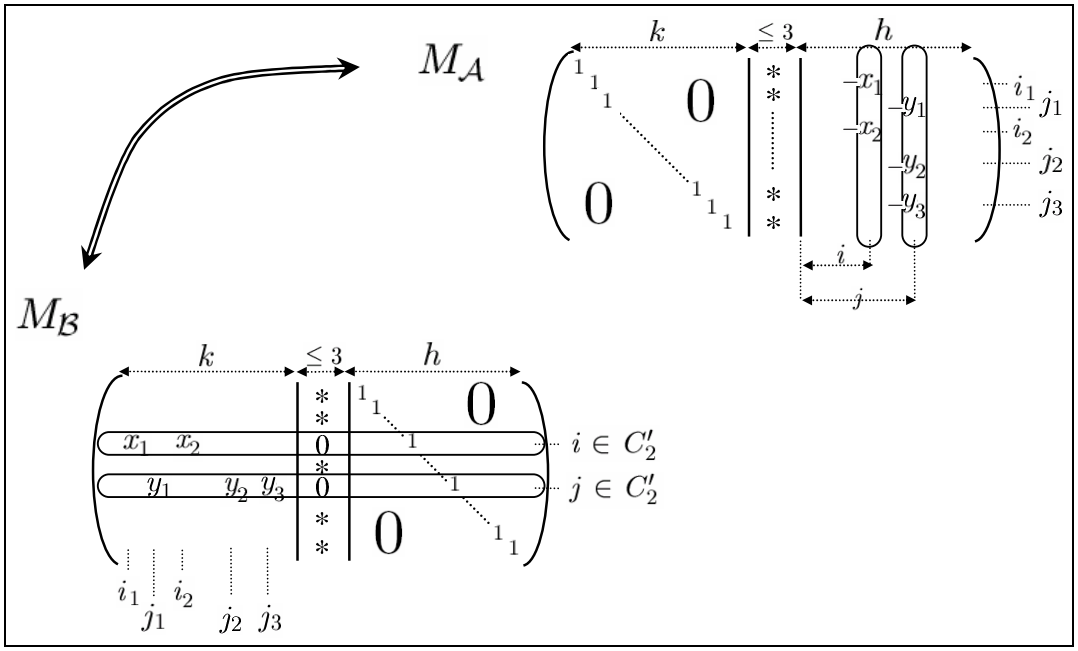

Figure 2: The duality between $M_{\mathcal{A}}$ and $M_{\mathcal{B}}$ when selected rows of $M_{\mathcal{B}}$ have 0 entries in columns $\{k+1, \ldots, n-h\}$.

C_2 contain more than 2 non-zero entries. First, recall that $k + h \geq n - 3$ and that each column contains at most one non-zero value in the rows of C_2. Thus, we can remove at most 3 rows from C_2 and obtain a set C_2', each remaining row of which does not contain non-zero entries in indices $k+1, \ldots, n-h$. Second, suppose rows $i, j \in C_2'$ each contains more than 2 non-zero entries. Let $i_1, \ldots, i_r \in [k]$, $r \geq 2$, denote the indices of the non-zero entries of row i excluding its value of 1 at index $n-h+i$ (recall that columns $n-h+1, \ldots, n$ of $M_{\mathcal{B}}$ form the identity matrix of order h). Similarly, let $j_1, \ldots, j_m \in [k]$, $m \geq 2$, denote the corresponding indices of row j :

$$(M_{\mathcal{B}})_{i,i_t} \neq 0 \text{ for } 1 \leq t \leq r \ , \ (M_{\mathcal{B}})_{i,n-h+i} = 1 \ ,$$

$$(M_{\mathcal{B}})_{j,j_t} \neq 0 \text{ for } 1 \leq t \leq m \ , \ (M_{\mathcal{B}})_{j,n-h+j} = 1 \ .$$

Since the rows of $M_{\mathcal{A}}$ are orthogonal to the rows of $M_{\mathcal{B}}$, and columns $1, \ldots, k$ of $M_{\mathcal{A}}$ form the identity matrix of order k, we deduce that:

$$(M_{\mathcal{A}})_{i_t,n-h+ii} \neq 0 \text{ for } 1 \leq t \leq r \ ,$$

$$(M_{\mathcal{A}})_{j_t,n-h+j} \neq 0 \text{ for } 1 \leq t \leq m \ .$$

See Figure 2 for an illustration of the above relation between $M_{\mathcal{A}}$ and $M_{\mathcal{B}}$. As the sets $\{i_1, \ldots, i_r\}$ and $\{j_1, \ldots, j_m\}$ are disjoint, columns $n-h+i$ and $n-h+j$ of $M_{\mathcal{A}}$ each contains at least 2 non-zero entries in pairwise distinct indices. In general, if m rows in C_2' contain more than 2 non-zero entries, we deduce that m columns in $M_{\mathcal{A}}$ contain at least 2 non-zero entries in a cascading manner. As argued above, there are at most $O(1)$ such columns in $M_{\mathcal{A}}$, hence $m = O(1)$: let C_2''

denote the set C_2' after removing these m rows, and let $h' = |C_2''| = h - O(1)$. Each row of C_2'' is in $\{0, \pm 1\}^n \setminus \{0,1\}^n$ and contains at most 2 non-zero values, and we deduce that without loss of generality:

$$M_{\mathcal{B}} = \left(\begin{array}{c|c|c|c|c} \overset{\leftarrow\cdots k \cdots\rightarrow}{-I_{h'}} & \overset{||\leftarrow\leq 3\rightarrow||}{0} & \overset{\leftarrow\cdots h \cdots\rightarrow}{0} & I_{h'} & 0 \\ * & * & * & 0 & I_{h-h'} \end{array} \right) . \tag{49}$$

Since the rows of $M_{\mathcal{A}}$ and $M_{\mathcal{B}}$ are orthogonal, it follows that:

$$M_{\mathcal{A}} = \left(\begin{array}{c|c|c|c|c} \overset{\leftarrow\cdots k \cdots\rightarrow}{I_{h'}} & \overset{||\leftarrow\leq 3\rightarrow||}{0} & \overset{\leftarrow\cdots h \cdots\rightarrow}{*} & I_{h'} & * \\ 0 & I_{k-h'} & * & 0 & * \end{array} \right) . \tag{50}$$

The above structure of $M_{\mathcal{A}}$ and $M_{\mathcal{B}}$ provides an upper bound on ℓ in terms of k, which we prove in Subsection 6.1:

Claim 6.1. *Let $\mathcal{A}$ and $\mathcal{B}$ be as above. If $|\mathcal{A}||\mathcal{B}| = \Omega(2^n/\sqrt{n})$, then:*

$$\ell \leq \left(\frac{1}{2} + o(1) \right) k \ . \tag{51}$$

The proof of the lemma is completed by the next two claims, which are proved in Subsections 6.2 and 6.3:

Claim 6.2. *Let $\mathcal{A}$ and $\mathcal{B}$ be as above. If $r_A = o(n)$ then $|\mathcal{A}||\mathcal{B}| \leq \binom{2\ell}{\ell} 2^{n-2\ell}$. Furthermore, equality holds iff (26) holds.*

Claim 6.3. *Let $\mathcal{A}$ and $\mathcal{B}$ be as above. If $r_A = \Omega(n)$ then the pair $\mathcal{A}, \mathcal{B}$ is suboptimal.*

6.1 Proof of Claim 6.1

Fix a choice of coefficients for the rows $h'+1, \ldots, h$ of $M_{\mathcal{B}}$, and let w_B denote the result of adding this combination to χ_{B_1}. As argued in the proof of Claim 5.1, the structure of $M_{\mathcal{B}}$ in (49) implies that each index $j \in [h']$ such that

$$w_B^{(j)} \neq 1 - w_B^{(n-h+j)} \tag{52}$$

eliminates at least one of the two possible coefficients for the row j of $M_{\mathcal{B}}$ (compare this to the treatment of the vector w_A in (35)). Thus, if there are $\omega(1)$ such coefficients, then w_B allows at most $o(2^{h'})$ combinations of the remaining rows of $M_{\mathcal{B}}$ to produce sets in $\mathcal{B}$. Since $|\mathcal{A}| = O(2^k/\sqrt{n})$ (recall that $r_A + s_A = \Omega(n)$), summing over at most $2^{h-h'}$ combinations for such vectors w_B gives $o(2^{k+h}/\sqrt{n})$ pairs $(A, B) \in \mathcal{A} \times \mathcal{B}$.

It remains to treat vectors w_B in which at most $O(1)$ indices $j \in [h']$ satisfy (52). Note that each $B \in \mathcal{B}$ produced from w_B and a combination of rows $1, \ldots, h'$ of $M_{\mathcal{B}}$ satisfies:

$$|B \cap \{j, n-h+j\}| = 1 \text{ for all but at most } O(1) \text{ indices } j \in [h'] \ . \tag{53}$$

Let $A \in \mathcal{A}$, and let $X_i \in \{0,1\}$ denotes the coefficient of the row i of $M_{\mathcal{A}}$ in the linear combination which produces A. By (53) and the structure of $M_{\mathcal{A}}$ in (50), we obtain that:

$$\left|A \cap B \cap \left([h'] \cup \{n-h+1,\ldots,n-h+h'\}\right)\right| = (\sum_{i=1}^{h'} X_i) + O(1) \ . \tag{54}$$

Furthermore, the structure of $M_{\mathcal{A}}$ in (50) gives:

$$\left|A \cap B \cap \{h'+1,\ldots,k\}\right| \leq \left|A \cap \{h'+1,\ldots,k\}\right| = \sum_{i=h'+1}^{k} X_i \ . \tag{55}$$

Combining (54) and (55) with the fact that $k + h' = n - O(1)$, we obtain that:

$$\ell = |A \cap B| \leq \left(\sum_{i=1}^{k} X_i\right) + O(1) \ .$$

Let $\varepsilon > 0$, and assume that $\ell > (1+\varepsilon)\frac{k}{2}$. By the Chernoff bound, the number of assignments of $\{0,1\}$ to the variables $X_1,\ldots,X_k$, which satisfy $\sum_{i=1}^{k} X_i > (1+\varepsilon)\frac{k}{2}$, is at most $2^k/\exp(\Omega(k)) = 2^k/\exp(\Omega(n))$. Therefore, the assumption on ℓ implies that at most $O(2^k/\exp(\Omega(n)))$ sets $A \in \mathcal{A}$ satisfy $|A \cap B| = \ell$, and summing over all sets B whose vector w_B is as above gives at most $2^{k+h}/\exp(\Omega(n))$ pairs $(A,B) \in \mathcal{A} \times \mathcal{B}$. This contradicts the assumption that $|\mathcal{A}||\mathcal{B}| = \Omega(2^n/\sqrt{n})$, and we conclude that $\ell \leq (\frac{1}{2} + o(1))k$, as required. ■

6.2 Proof of Claim 6.2

The assumptions $r_A + s_A = \Omega(n)$ and $r_A = o(n)$ imply that $s_A = \Omega(n)$, and, as before, we may assume that $r_A = O(1)$, otherwise we get $|\mathcal{A}| = o(2^k/\sqrt{n})$, leading to a suboptimal pair $\mathcal{A},\mathcal{B}$. Thus, each column of $M_{\mathcal{A}}$ has at most $O(1)$ non-zero entries. Since $n-(k+h) \leq 3$ and $h - h' = O(1)$, it follows that at most $O(1)$ rows of $M_{\mathcal{A}}$ have non-zero entries in columns $\{k+1,\ldots,n-h\} \cup \{n-h+h'+1,\ldots,n\}$. Without loss of generality, reorder the indices of these rows to $k'+1,\ldots,k$ (where $k' = k - O(1)$), and let $h'' = h' - O(1)$ reflect the reordering of rows whose original indices belonged to $[h']$. We obtain that:

$$M_{\mathcal{A}} = \overset{\overset{\leftarrow\cdots\cdots\ k\ \cdots\cdots\rightarrow}{\overset{\leftarrow\cdots\cdots\ k'\ \cdots\rightarrow}{\overset{\leftarrow\cdots\ h''\ \cdots\rightarrow}{\left(\begin{array}{c|c|c|c|c|c} I_{h''} & 0 & 0 & 0 & I_{h''} & 0 \\ 0 & I_{k'-h''} & 0 & 0 & 0 & 0 \\ 0 & 0 & I_{k-k'} & * & 0 & * \end{array}\right)}}}{\overset{\leftarrow\cdots\ h'\ \cdots\rightarrow}{\overset{\leftarrow\cdots\ h\ \cdots\rightarrow}{\overset{\leftarrow\cdots\ \leq 3\ \cdots\rightarrow}{}}}} \ , \tag{56}$$

and by the orthogonality of $M_{\mathcal{A}}$ and $M_{\mathcal{B}}$:

$$M_{\mathcal{B}} = \overset{\overset{\leftarrow\cdots\ k'\ \cdots\rightarrow}{\overset{\leftarrow\cdots\ h''\ \cdots\rightarrow}{\overset{\leftarrow\cdots\ O(1)\ \cdots\rightarrow}{}}}}{\left(\begin{array}{c|c|c|c|c} -I_{h''} & 0 & 0 & I_{h''} & 0 \\ 0 & 0 & * & 0 & I_{h-h''} \end{array}\right)} \ . \tag{57}$$

Notice that the first k' rows of $M_{\mathcal{A}}$ form an antichain on the first k' elements, hence:

$$|\mathcal{A}| \leq (1+o(1))\frac{2^k}{\sqrt{\pi k'/2}} \leq (1+o(1))\frac{2^k}{\sqrt{\pi \ell}} \ ,$$

where the last inequality is by (51). This yields an upper bound on $|\mathcal{A}||\mathcal{B}|$ which is asymptotically tight, hence any additional constant factor bounded away from 1 which multiplies either $|\mathcal{A}|$ or $|\mathcal{B}|$ implies that the pair $(\mathcal{A},\mathcal{B})$ is suboptimal. In particular:

(i) If $k+h<n$, we have a suboptimal pair: $|\mathcal{A}||\mathcal{B}| \leq \left(\frac{1}{2}+o(1)\right)2^n/\sqrt{\pi\ell}$. Assume therefore that $k+h=n$.

(ii) If $M_{\mathcal{B}}$ has a column with more than 1 non-zero entry, we gain a multiplicative factor of at most $\frac{3}{4}$ and we are done. The same applies to $M_{\mathcal{A}}$: such a column has $O(1)$ non-zero entries, as $r_A = O(1)$, and once we set the combination of these rows (gaining a factor of at most $\frac{3}{4}$) as well as the other rows left in $\{k'+1,\ldots,k\}$, the combination of the remaining rows $[k']$ must still form an antichain.

(iii) If $M_{\mathcal{A}}$ has a row with more than 2 non-zero entries, by Item (i) it corresponds to a column with more than 1 non-zero entry in $M_{\mathcal{B}}$ (since statement (41) holds), which does not exist according to Item (ii). The same applies to the rows of $M_{\mathcal{B}}$.

(iv) Each row of $M_{\mathcal{B}}$ must belong to $\{0,\pm 1\}^n \setminus \{0,1\}^n$, otherwise the arguments of Claim 3.4 imply a constant multiplicative factor of at most $\frac{1}{2}$.

Items (iii) and (iv) imply that every row of $M_{\mathcal{B}}$ has precisely two non-zero entries: $\{1,-1\}$, and without loss of generality, $h''=h$. Recalling (56) and (57), $M_{\mathcal{A}}$ and $M_{\mathcal{B}}$ take the following form:

$$\begin{aligned} M_{\mathcal{A}} &= \left(\begin{array}{c|c|c} I_h & 0 & I_h \\ 0 & I_{k-h} & 0 \end{array}\right) , \\ M_{\mathcal{B}} &= \left(\begin{array}{c|c|c} -I_h & 0 & I_h \end{array}\right) . \end{aligned} \tag{58}$$

Notice that the above structure of $M_{\mathcal{B}}$ implies that $\chi_B^{(j)} = \chi_{B_1}^{(j)}$ for all $j \in \{h+1,\ldots,k\}$ and $B \in \mathcal{B}$. As we assumed in (20) that $\bigcup_{B\in\mathcal{B}} \mathcal{B} = [n]$, it follows that $\{h+1,\ldots,k\} \subset B_1$.

Consider the rows of $M_{\mathcal{B}}$, let w_B be initially set to the value of the vector χ_{B_1}, then subtract from w_B each row i of $M_{\mathcal{B}}$ for which $k+i \in B_1$. This translates the possible coefficients for each row i of $M_{\mathcal{B}}$ to $\{0,1\}$; hence, the characteristic vector of every element of $\mathcal{B}$ is a sum of w_B with a sub-sum of the rows of $M_{\mathcal{B}}$. First, $w_B^{(j)} = \chi_{B_1}^{(j)} = 1$ for all $j \in \{h+1,\ldots,k\}$. Second, the structure of $M_{\mathcal{B}}$ (58) implies that, if $w_B^{(j)} \neq 1$ for some $j \in [h]$, then row j cannot be added to w_B to yield a vector in $\{0,1\}^n$. Since this leads to a suboptimal pair $(\mathcal{A},\mathcal{B})$ (of size at most $(\frac{1}{2}+o(1))2^n/\sqrt{\pi\ell}$), we deduce that:

$$w_B = \big(\overbrace{1\ldots1}^{k}\ \overbrace{0\ldots0}^{h}\big) \ .$$

The structure of $M_{\mathcal{B}}$ (58) implies that for every $B \in \mathcal{B}$, χ_B is of the form:

$$\chi_B = \big(\overbrace{0/1\ldots0/1}^{h}\ \overbrace{1\ldots1}^{k-h}\ \overbrace{1/0\ldots1/0}^{h}\big)\ ,$$

where precisely one index in each of the pairs $\{(1,k+1),\ldots,(h,k+h)\}$ is equal to 1 in χ_B. If $X_i \in \{0,1\}$ denotes the coefficient of row i of $M_{\mathcal{A}}$ in a combination that produces some $A \in \mathcal{A}$, it follows from (58) that $\ell = |A \cap B| = \sum_{i=1}^{k} X_i$ for all $B \in \mathcal{B}$. By the properties of the binomial distribution, we deduce that $|\mathcal{A}| \leq \binom{k}{\ell}$, and altogether:

$$|\mathcal{A}||\mathcal{B}| \leq 2^{n-k}\binom{k}{\ell}\ .$$

The expression above realizes the bound (3) iff either $k = 2\ell$ or $k = 2\ell - 1$, hence the final structure of the optimal pair $(\mathcal{A},\mathcal{B})$ is as described in Lemma 4.2. ■

6.3 Proof of Claim 6.3

The assumption $r_A = \Omega(n)$ implies that, unless $s_A = O(1)$, we get $|\mathcal{A}| = o(2^k/\sqrt{k}) = o(2^k/\sqrt{n})$ as required. However, if we remove the rows R_A from $[k]$, (50) implies that only the columns $\{k+1,\ldots,n-h\} \cup \{n-h+h'+1,\ldots,n\}$ can contribute -1 entries to the remaining rows, and each column has at most 1 non-zero entry in each of these rows. Since $n-(k+h) \leq 3$ and $h - h' = O(1)$, we deduce that $[k] - r_A - s_A = O(1)$, and altogether:

$$r_A = k - O(1)\ .$$

Definition. *A column of $M_{\mathcal{A}}$ is called "heavy" if it contains $k - O(1)$ non-zero entries.*

The next argument shows that there exists a heavy column in $M_{\mathcal{A}}$. There are at most $O(1)$ columns which may contain more than 1 non-zero entry in $M_{\mathcal{A}}$ (as all the columns $[k]$ as well as $\{n-h+1,\ldots,n-h+h'\}$ contain a single non-zero entry of 1). Therefore, there exists some column $q \in [n]$ of $M_{\mathcal{A}}$ with $\Omega(r_A) = \Omega(k)$ non zero entries. If some other column has $\omega(1)$ non-zero entries in a cascading manner, we obtain $|\mathcal{A}| = o(2^k/\sqrt{n})$, and we are done. We deduce that column q has $r_A - O(1) = k - O(1)$ non-zero entries, therefore column q is heavy. Applying the Littlewood-Offord Lemma to the $k - O(1)$ rows where column q is non-zero at, we obtain that:

$$|\mathcal{A}| \leq (2+o(1))\frac{2^k}{\sqrt{\pi k/2}} \leq (2+o(1))\frac{2^k}{\sqrt{\pi\ell}}\ , \tag{59}$$

where the last inequality is by (51).

Let q denote a heavy column of $M_{\mathcal{A}}$. Lemma 2.3 enables us to eliminate the case where all non-zero entries of q are ± 1. To see this, assume the converse, and let:

$$U = \{i \in [k] : (M_{\mathcal{A}})_{i,q} = 1\}\ ,\ V = \{i \in [k] : (M_{\mathcal{A}})_{i,q} = -1\}\ .$$

Recall that $|U| + |V| = k - O(1)$, and take $\varepsilon > 0$. If $|U| \geq (\frac{1}{2} + \varepsilon)k$, then Chernoff's bound implies that the number of sub-sums of the rows $U \cup V$ which give a value of $\{0, 1\}$ in this column is at most $2^k / \exp(\Omega(k))$. We deduce that $|U| = (\frac{1}{2} + o(1))k$ and that $|V| = (\frac{1}{2} + o(1))k$.

Set $m = n - (k + h) + (h - h') = O(1)$. For each possible values $\underline{x} \in \{0, 1\}^m$ for the output of columns $\{k + 1, \ldots, n - h\} \cup \{n - h + h' + 1, \ldots, n\}$, the family of all sets $A \in \mathcal{A}$ that match the pattern $\underline{x}$ in the above set of columns (that is, $k + j \in A$ iff $x_j = 1$ for $j \in \{1, \ldots, n - h - k\}$ and so on) is an antichain, and either $|A \cap V| = |A \cap U|$ or $|A \cap V| = |A \cap U| - 1$ (that is because if $j \in A$ for some $j \in [k]$ then the linear combination producing A assigns a coefficient 1 to row j, which then contributes either 1, -1 or 0 at column q, depending on whether $j \in U$, $j \in V$ or $j \in [k] \setminus (U \cup V)$ respectively). Thus, Lemma 2.3 implies that $|\mathcal{A}| = O(2^k/k) = O(2^k/n)$. We may therefore assume that:

$$\text{Every heavy column } q \text{ of } M_{\mathcal{A}} \text{ satisfies } (M_{\mathcal{A}})_{i,q} \notin \{0, \pm 1\} \text{ for some } i \in [k] \ . \tag{60}$$

This provides an upper bound on $|\mathcal{B}|$:

$$|\mathcal{B}| \leq 2^{n-k-1} \ . \tag{61}$$

The above bound follows immediately if $h < n - k$, so consider the case $k + h = n$, and let q denote a heavy column of $M_{\mathcal{A}}$. By the orthogonality of $M_{\mathcal{A}}, M_{\mathcal{B}}$, (41) holds, and (60) now implies that $(M_{\mathcal{B}})_{q-k,i} \notin \{0, \pm 1\}$ for some $i \in [k]$. In particular, row $q - k$ of $M_{\mathcal{B}}$ does not belong to $\{0, \pm 1\}^n$, and hence $|\mathcal{B}| \leq 2^{h-1}$ (as enumerating on the coefficients for rows $[h] \setminus \{q - k\}$ of $M_{\mathcal{B}}$ leaves at most one legal coefficient for row $q - k$).

Combining (61) with (59) yields an asymptotically tight upper bound on $|\mathcal{A}||\mathcal{B}|$:

$$|\mathcal{A}||\mathcal{B}| \leq (1 + o(1))\frac{2^n}{\sqrt{\pi k/2}} \leq (1 + o(1))\frac{2^n}{\sqrt{\pi \ell}} \ .$$

Let $\varepsilon > 0$; if $k \geq (2 + \varepsilon)\ell$, then the first inequality of the bound above implies that the pair $\mathcal{A}, \mathcal{B}$ is suboptimal. Therefore, adding this to (51), we may assume that:

$$k = (2 + o(1))\ell \ . \tag{62}$$

Next, we wish to eliminate the case where some column q has $k - O(1)$ non-zero entries, all of which have the same sign. In this case, let $Q = \{i : (M_{\mathcal{A}})_{i,q} \neq 0\}$. As all the entries in rows Q and column q of $M_{\mathcal{A}}$ have the same sign, only the all-zero linear combination of these rows can produce the value 0 at index q. Applying the Littlewood-Offord Lemma to the rows Q, we obtain an upper bound on the number of combinations which produce the value 1, and altogether:

$$|\mathcal{A}| \leq 2^{k-|Q|}(\binom{|Q|}{\lfloor |Q|/2 \rfloor} + 1) = (1 + o(1))\frac{2^k}{\sqrt{\pi \ell}} \ ,$$

where in the last equality we used the fact that $|Q| \geq (2 + o(1))\ell$, as $|Q| = k - O(1)$. By (61), this implies that $|\mathcal{A}||\mathcal{B}| \leq (\frac{1}{2} + o(1))2^n/\sqrt{\pi \ell}$, implying the statement of the claim. We thus assume that:

$$\text{Every heavy column } q \text{ of } M_{\mathcal{A}} \text{ contains both positive and negative entries} \ . \tag{63}$$

Using the last statement, we prove the next claim:

Claim 6.4. *Let $\lambda \in \{0,1\}$, $L \subset [k]$ and $d > 0$, and let q denote a heavy column of $M_{\mathcal{A}}$. Define:*

$$\mathcal{A}^{(q)}_{L,d,\lambda} = \{A \in \mathcal{A} : |A \cap L| = d \ , \chi^{(q)}_A = \lambda\} \ . \tag{64}$$

If $d = (1+o(1))\ell$ and $|L| \geq (1+o(1))\ell$ then:

$$|\mathcal{A}^{(q)}_{L,d,\lambda}| \leq \left(\frac{3}{4} + o(1)\right) \frac{2^k}{\sqrt{\pi\ell}} \ . \tag{65}$$

Proof. Let Q denote the indices of the rows in which column q of $M_{\mathcal{A}}$ has a non-zero entry. Observe that if $Q \nsubseteq L$, then the rows of L have at most $\binom{|L|}{d}$ legal combinations, and the remaining rows $[k] \setminus L$ have at most $2^{k-|L|-1}$ legal combinations, as these rows contain non-zero entries in column q, which must combine to a final value of λ. Hence, in this case:

$$|\mathcal{A}^{(q)}_{L,d,\lambda}| \leq \frac{1}{2} \cdot 2^{k-|L|}\binom{|L|}{d} \leq \frac{1}{2}2^{k-|L|}\binom{|L|}{\lfloor |L|/2 \rfloor} = \frac{1+o(1)}{2} \cdot \frac{2^k}{\sqrt{\pi|L|/2}} \leq \left(\frac{1}{\sqrt{2}} + o(1)\right)\frac{2^k}{\sqrt{\pi\ell}} \ ,$$

where the last inequality is by the fact that $|L| \geq (1+o(1))\ell$. Assume therefore that $Q \subset L$, and notice that, as $|Q| = k - O(1)$ and $L \subset [k]$, then $|L| = k - O(1)$, and by (62):

$$|L| = (2+o(1))\ell = (2+o(1))d \ .$$

Fix an enumeration on the coefficients of the rows $[k] \setminus L$, and let $\mathcal{S} \subset 2^L$ denote the d-element subsets of the rows of L which extend this enumeration to elements of $\mathcal{A}^{(q)}_{L,d,\lambda}$. Let $j_1, j_2 \in L$ be two indices such that $(M_{\mathcal{A}})_{j_1,q} \neq (M_{\mathcal{A}})_{j_2,q}$ (such indices exist by (63) and since $Q \subset L$), and define:

$$\mathcal{S}_0 = \{S \subset [L] : |S| = d \ , \ |S \cap \{j_1, j_2\}| = 1\} \ .$$

Notice that, as $j_1 \neq j_2$, the function $f : \mathcal{S}_0 \to \mathcal{S}_0$ which swaps j_1, j_2 is a bijection, which satisfies the following property for all $S \in \mathcal{S}_0$: at most one of the subsets $\{S, f(S)\}$ can belong to $\mathcal{S}$. Furthermore, if S is a random d-element set of L, then:

$$\Pr[S \in \mathcal{S}_0] = \frac{2\binom{|L|-2}{d-1}}{\binom{|L|}{d}} = \frac{2d(|L|-d)}{|L|(|L|-1)} = \frac{1}{2} + o(1) \ ,$$

and thus $|\mathcal{S}_0| = (\frac{1}{2} + o(1))\binom{|L|}{d}$, and we deduce that:

$$|\mathcal{S}| \leq \binom{|L|}{d} - \frac{|\mathcal{S}_0|}{2} = \left(\frac{3}{4} + o(1)\right)\binom{|L|}{d} \ .$$

Therefore:

$$|\mathcal{A}^{(q)}_{L,d,\lambda}| \leq 2^{k-|L|}|\mathcal{S}| \leq \left(\frac{3}{4} + o(1)\right)\frac{2^k}{\sqrt{\pi|L|/2}} = \left(\frac{3}{4} + o(1)\right)\frac{2^k}{\sqrt{\pi\ell}} \ ,$$

as required. ■

In order to deduce the claim from (65), we treat the two cases $k+h<n$ and $k+h=n$ in Claims 6.5 and 6.6 below.

Claim 6.5. *Let $\mathcal{A},\mathcal{B}$ be as above. If $k+h<n$, then the pair $\mathcal{A},\mathcal{B}$ is suboptimal.*

Proof. In this case, we may assume that $k+h=n-1$, otherwise (59) implies that $|\mathcal{A}||\mathcal{B}| \leq (\frac{1}{2}+o(1))2^n/\sqrt{\pi\ell}$. Recalling (49) and (50), we have:

$$M_{\mathcal{A}} = \begin{array}{c} \overset{\leftarrow\!-\!-\cdots k\cdots-\!-\!\rightarrow}{} \\ \left(\begin{array}{c|c|c|c|c} I_{h'} & 0 & * & I_{h'} & * \\ 0 & I_{k-h'} & * & 0 & * \end{array}\right) \end{array} \quad \begin{array}{c} \overset{\leftarrow\!-\!-1\!-\!\rightarrow}{} \\ \end{array} \quad \begin{array}{c} \overset{\leftarrow\!-\!-\cdots h\cdots-\!-\!\rightarrow}{} \\ \end{array}$$

$$M_{\mathcal{B}} = \begin{array}{c} \overset{\leftarrow\!-\!-\cdots k\cdots-\!-\!\rightarrow}{} \\ \left(\begin{array}{c|c|c|c|c} -I_{h'} & 0 & 0 & I_{h'} & 0 \\ * & * & * & 0 & I_{h-h'} \end{array}\right) \end{array} \quad \begin{array}{c} \overset{\leftarrow\!-\!-1\!-\!\rightarrow}{} \\ \end{array} \quad \begin{array}{c} \overset{\leftarrow\!-\!-\cdots h\cdots-\!-\!\rightarrow}{} \\ \end{array} \qquad (66)$$

Let $m=h-h'=O(1)$, and consider a choice of coefficients for rows $h'+1,\ldots,h$ of $M_{\mathcal{B}}$, yielding (together with χ_{B_1}) a vector w_B. First, by (59), each of the 2^m-1 choices of coefficients such that $(w_B^{(n-m+1)}\ldots w_B^{(n)}) \neq 0$ can each be completed to a pair $(A,B)\in\mathcal{A}\times\mathcal{B}$, in at most

$$2^{h-m}\cdot(2+o(1))\frac{2^k}{\sqrt{\pi\ell}} = (1+o(1))\frac{2^{n-m}}{\sqrt{\pi\ell}}$$

ways. Let $\mathcal{B}_0$ denote the sets $B\in\mathcal{B}$ which can be produced from the remaining combination for w_B (the one for which $w_B^{(n-m+1)}=\ldots=w_B^{(n)}=0$). In order to show that $\mathcal{A},\mathcal{B}$ is suboptimal, it is enough to show that:

$$|\mathcal{A}||\mathcal{B}_0| \leq (\alpha+o(1))\frac{2^{n-m}}{\sqrt{\pi\ell}} \text{ for some } \alpha<1\ , \qquad (67)$$

since this would imply:

$$|\mathcal{A}||\mathcal{B}| \leq (2^m-1)(1+o(1))\frac{2^{n-m}}{\sqrt{\pi\ell}} + (\alpha+o(1))\frac{2^{n-m}}{\sqrt{\pi\ell}} = \left(1-\frac{1-\alpha}{2^m}+o(1)\right)\frac{2^n}{\sqrt{\pi\ell}}\ . \qquad (68)$$

If for some index $j\in[h']$ we have $w_B^{(n-h+j)}\neq 1-w_B^{(j)}$, then row j of $M_{\mathcal{B}}$ has at most one legal coefficient, hence $|\mathcal{B}_0|\leq 2^{h-m-1}$, and the same holds in case $w_B\notin\{0,1\}^n$ (if $j\in\{h'+1,\ldots,n-h\}$ is such that $w_B^{(j)}\notin\{0,1\}$, then $\mathcal{B}_0=\emptyset$). As $|\mathcal{A}|\leq(2+o(1))\frac{2^k}{\sqrt{\pi\ell}}$ and $k+h<n$, it follows that in the above two cases $|\mathcal{A}||\mathcal{B}_0|\leq\left(\frac{1}{2}+o(1)\right)\frac{2^{n-m}}{\sqrt{\pi\ell}}$, satisfying (67) for $\alpha=\frac{1}{2}$.

Assume therefore that $w_B^{(n-h+j)}=1-w_B^{(j)}$ for all $j\in[h']$, and that $w_B\in\{0,1\}^n$, and define:

$$L=[h']\cup\{h'+1\leq i\leq k : w_B^{(i)}=1\}\ .$$

Recalling that $w_B^{(n-h+h'+1)}=\ldots=w_B^{(n)}=0$, (66) implies that every B produced from w_B satisfies:

$$\ell=|A\cap B|=\mathbf{1}_{\{k+1\in A\cap B\}}+\sum_{i\in L}X_i\ , \qquad (69)$$

for all $A \in \mathcal{A}$, where $X_i \in \{0,1\}$ denotes the coefficient for row i in a combination which produces A from $M_{\mathcal{A}}$. We may assume that $\mathcal{B}_0 \neq \emptyset$ (otherwise (67) immediately holds), and by (69) we obtain that $|L| \geq \ell - 1$, and in particular, $|L| \geq (1 + o(1))\ell$.

If column $k+1$ of $M_{\mathcal{A}}$ has $o(k) = o(|L|)$ non-zero entries in some rows U, fix an enumeration on the coefficients of these rows, and let $L' = L \setminus U$, noting that $|L'| = (1 - o(1))|L| \geq (1 - o(1))\ell$. The enumeration on the coefficients for the rows U determines whether or not $k+1 \in A \cap B$, and by (69), this determines the value of $\sum_{i \in L'} X_i$. Therefore, by the properties of the binomial distribution, there are at most $\binom{|L'|}{\lfloor |L'|/2 \rfloor} \leq 2^{|L'|}/\sqrt{\pi |L'|/2}$ combinations for the coefficients of the rows L'. We conclude that:

- In case $|L| \geq (1 - o(1))k$, recalling (62), we get $|\mathcal{A}| \leq (1 + o(1))\frac{2^k}{\sqrt{\pi \ell}}$.
- Otherwise, $k - |L| = \Omega(k)$, and after choosing a combination for the rows L', we are left with rows $[k] \setminus (L \cup U)$ which contain $\Omega(k)$ non-zero entries in some heavy column q of $M_{\mathcal{A}}$ (recall that each heavy column has $k - O(1)$ non-zero entries). The Littlewood-Offord Lemma gives a factor of $O(1/\sqrt{k})$ on the number of combinations for the remaining rows, which, when multiplied by the previous factor of $O(1/\sqrt{|L'|}) = O(1/\sqrt{k})$ gives $|\mathcal{A}| \leq O(2^k/k) = O(2^k/\ell)$. In particular, we have $|\mathcal{A}| \leq (1 + o(1))\frac{2^k}{\sqrt{\pi \ell}}$ (with room to spare).

Altogether, as $|\mathcal{B}_0| \leq 2^{h-m} \leq 2^{n-m-k-1}$, in both cases we obtain that (67) holds for $\alpha = \frac{1}{2}$.

It remains to treat the case where column $k+1$ of $M_{\mathcal{A}}$ has $\Omega(k)$ non-zero entries; by the arguments in the beginning of the proof of Claim 6.3, it follows that column $k+1$ is heavy. Therefore, recalling that $\mathcal{B}_0 \neq \emptyset$ and using the definition (64), it follows that:

$$|\mathcal{A}| = \begin{cases} |\mathcal{A}^{(k+1)}_{L,\ell,0}| + |\mathcal{A}^{(k+1)}_{L,\ell,1}| & \text{if } w_B^{(k+1)} = 0 \\ \\ |\mathcal{A}^{(k+1)}_{L,\ell,0}| + |\mathcal{A}^{(k+1)}_{L,\ell-1,1}| & \text{if } w_B^{(k+1)} = 1 \end{cases} .$$

Applying Claim 6.4 (recall that $|L| \geq \ell - 1$) gives:

$$|\mathcal{A}| \leq 2 \cdot \left(\frac{3}{4} + o(1)\right)\frac{2^k}{\sqrt{\pi \ell}} = \left(\frac{3}{2} + o(1)\right)\frac{2^k}{\sqrt{\pi \ell}} ,$$

and as $|\mathcal{B}_0| \leq 2^{h-m} \leq 2^{n-m-k-1}$, (67) holds for $\alpha = \frac{3}{4}$, as required. ■

Claim 6.6. *Let $\mathcal{A}, \mathcal{B}$ be as above. If $k + h = n$, then the pair $\mathcal{A}, \mathcal{B}$ is suboptimal.*

Proof. The proof will follow from arguments similar to those in the proof of Claim 6.5; the factor of $\frac{1}{2}$ which followed from the case $k + h < n$ is replaced by the duality between $M_{\mathcal{A}}, M_{\mathcal{B}}$ (41) when

$k + h = n$. The assumption $k + h = n$ gives (49) and (50) the following form:

$$M_{\mathcal{A}} = \left(\begin{array}{c|c|c|c} \overset{\leftarrow\cdots k \cdots\rightarrow}{I_{h'}} & \overset{\leftarrow\cdots k \cdots\rightarrow}{0} & \overset{\leftarrow\cdots h \cdots\rightarrow}{I_{h'}} & \overset{\leftarrow\cdots h \cdots\rightarrow}{*} \\ 0 & I_{k-h'} & 0 & * \end{array}\right) .$$

$$M_{\mathcal{B}} = \left(\begin{array}{c|c|c|c} \overset{\leftarrow\cdots k \cdots\rightarrow}{-I_{h'}} & \overset{\leftarrow\cdots k \cdots\rightarrow}{0} & \overset{\leftarrow\cdots h \cdots\rightarrow}{I_{h'}} & \overset{\leftarrow\cdots h \cdots\rightarrow}{0} \\ * & * & 0 & I_{h-h'} \end{array}\right)$$

Let $q \in [n]$ denote a heavy column of $M_{\mathcal{A}}$; by the above structure of $M_{\mathcal{A}}$, we can assume without loss of generality that $q = n$. Let $p \in [k]$ be such that $(M_{\mathcal{A}})_{p,n} \notin \{0, \pm 1\}$ (such a p exists by (60)). Recall that, as $k + h = n$, the orthogonality of $M_{\mathcal{A}}, M_{\mathcal{B}}$ implies that (41) holds, and thus $(M_{\mathcal{B}})_{h,p} = -(M_{\mathcal{A}})_{p,n} \notin \{0, \pm 1\}$.

Consider the following set of rows of $M_{\mathcal{B}}$:

$$W = \begin{cases} \{p\} \cup \{h' + 1, \ldots, h - 1\} & \text{if } p \in [h'] \ , \\ \{h' + 1, \ldots, h - 1\} & \text{otherwise} \ . \end{cases}$$

Let $m = |W|$, and consider one of the $2^m - 1$ choices of coefficients for the rows W of $M_{\mathcal{B}}$, such that the sum of χ_{B_1} and the resulting combination of these rows, satisfies $w_B^{(k+j)} \neq 0$ for some $j \in W$. Observe that w_B allows at most one coefficient for row h of $M_{\mathcal{B}}$, since all the remaining rows $[h-1] \setminus W$ have 0 entries at column p, whereas $(M_{\mathcal{B}})_{h,p} \notin \{0, \pm 1\}$. Therefore, by (59), each of the $2^m - 1$ possibilities for such vectors w_B can produce at most:

$$2^{h-m-1} \cdot (2 + o(1)) \frac{2^k}{\sqrt{\pi \ell}} = (1 + o(1)) \frac{2^{n-m}}{\sqrt{\pi \ell}}$$

pairs $(A, B) \in \mathcal{A} \times \mathcal{B}$. Consider the remaining combination of the rows W, satisfying $w_B^{(k+j)} = 0$ for all $j \in W$, and let $\mathcal{B}_0$ denote the sets $B \in \mathcal{B}$ which can be produced from w_B. Using this notation, it is enough to show that (67) holds, and the claim will follow from the resulting calculation (68).

As before, the fact that $(M_{\mathcal{B}})_{h,p} \notin \{0, \pm 1\}$ and that the remaining rows $[h-1] \setminus W$ have 0 entries in column p, implies that there is at most one coefficient possible for row h. If no coefficient for row h is legal, we get $\mathcal{B}_0 = \emptyset$ and (67) holds, otherwise let $\tilde{w}_B$ denote the sum of w_B with the appropriate multiple of row h of $M_{\mathcal{B}}$. We are left with $h - m - 1$ rows of $M_{\mathcal{B}}$ whose coefficients were not yet determined: rows $[h-1] \setminus W = [h'] \setminus \{p\}$.

If $\tilde{w}_B^{(j)} \neq 1 - \tilde{w}_B^{(k+j)}$ for some $j \in [h'] \setminus \{p\}$ or $\tilde{w}_B \neq \{0,1\}^n$, we obtain an additional factor of at most $\frac{1}{2}$ from one of the remaining rows of $M_{\mathcal{B}}$, and $|\mathcal{B}_0| \leq 2^{h-m-2}$. Combining this with (59) implies that (67) holds for $\alpha = \frac{1}{2}$. Assume therefore that $\tilde{w}_B^{(j)} = 1 - \tilde{w}_B^{(k+j)}$ for all $j \in [h'] \setminus \{p\}$ and that $\tilde{w}_B \in \{0,1\}^n$, and define:

$$L = [h'] \setminus \{p\} \cup \left\{ i \in \{h' + 1, \ldots, k\} \cup \{p\} : \tilde{w}_B^{(i)} = 1 \right\} \ .$$

Since every set B produced from $\tilde{w}_B$ satisfies $|B \cap \{j, k+j\}| = 1$ for all $j \in [h'] \setminus \{p\}$ and $k+j \notin B$ for all $j \in W$, we deduce that, if $p \notin [h']$ (in which case $W = \{h'+1, \ldots, h-1\}$):

$$\ell = |A \cap B| = \mathbf{1}_{\{n \in A \cap B\}} + \sum_{i \in L} X_i \ , \tag{70}$$

for all $A \in \mathcal{A}$, where $X_i \in \{0,1\}$ denotes the coefficient for row i in a combination which produces A from $M_{\mathcal{A}}$. On the other hand, if $p \in [h']$, then $p \in W$ and it follows that $\tilde{w}_B^{(k+p)} = 0$, and:

- If $\tilde{w}_B^{(p)} = 0$, then $p \notin L$, and indeed, X_p does not contribute to $|A \cap B|$ for all $A \in \mathcal{A}$ and B produced by $\tilde{w}_B$, as neither p nor $k+p$ belong to B.
- If $\tilde{w}_B^{(p)} = 1$, then $p \in L$, and indeed X_p contributes 1 to $|A \cap B|$ for all $A \in \mathcal{A}$ and B produced by $\tilde{w}_B$, as $p \in B$ and $k+p \notin B$.

We deduce that (70) holds for $p \in [h']$ as-well. Recalling that $\mathcal{B}_0 \neq \emptyset$ (otherwise (67) immediately holds) (70) gives $|L| \geq \ell - 1$, and in particular, $|L| \geq (1+o(1))\ell$. Using the definition (64), it follows that:

$$|\mathcal{A}| = \begin{cases} |\mathcal{A}^{(n)}_{L,\ell,0}| + |\mathcal{A}^{(n)}_{L,\ell,1}| & \text{if } \tilde{w}_B^{(n)} = 0 \\ \\ |\mathcal{A}^{(n)}_{L,\ell,0}| + |\mathcal{A}^{(n)}_{L,\ell-1,1}| & \text{if } \tilde{w}_B^{(n)} = 1 \end{cases} .$$

Applying Claim 6.4 (recall that $|L| \geq \ell - 1$) gives:

$$|\mathcal{A}| \leq 2 \cdot \left(\frac{3}{4} + o(1)\right) \frac{2^k}{\sqrt{\pi \ell}} = \left(\frac{3}{2} + o(1)\right) \frac{2^k}{\sqrt{\pi \ell}} \ ,$$

and as $|\mathcal{B}_0| \leq 2^{h-m-1}$, (67) holds for $\alpha = \frac{3}{4}$, as required. ■

This completes the proof of Claim 6.3 and of Lemma 4.2.

7 Concluding remarks and open problems

- We have shown that if two families of subsets of an n-element set, $\mathcal{A}, \mathcal{B}$, are ℓ-cross-intersecting, and ℓ is sufficiently large, then $|\mathcal{A}||\mathcal{B}| \leq \binom{2\ell}{\ell} 2^{n-2\ell}$, and in addition, we have given a complete characterization of all the extremal pairs $\mathcal{A}, \mathcal{B}$ for which equality is achieved.
- It would be interesting to prove that the above result holds for all values of ℓ (instead of all $\ell \geq \ell_0$ for some ℓ_0). Perhaps knowing the precise structure of the extremal pairs $\mathcal{A}, \mathcal{B}$, as described in Theorem 1.1 (assuming that this holds for all ℓ), will assist in proving this result.
- Finally, one may consider the corresponding problem where the pair $\mathcal{A}, \mathcal{B}$ does not have one possible cross-intersection, but rather a set L of legal cross-intersections. Such notions have been studied in [1], [17], [12], with different restrictions on L, and it would be interesting to derive tight bounds on $|\mathcal{A}||\mathcal{B}|$, and possibly describe the structure of all the extremal pairs, when in addition, each member of L is larger than some predefined integer ℓ.

Acknowledgement The authors wish to thank Benny Sudakov for useful discussions, as well as an anonymous referee for a careful reading of an earlier version.

References

[1] R. Ahlswede, N. Cai, and Z. Zhang, A general 4-words inequality with consequences for 2-way communication complexity, Adv. in Appl. Math. 10 (1989), 75-94.

[2] N. Alon and J. H. Spencer, *The Probabilistic Method*, Second Edition, Wiley, New York, 2000.

[3] L. Babai and P. Frankl, *Linear Algebra Methods in Combinatorics*, Preliminary Version 2. Dept. of Computer Science, The Univesity of Chicago, 1992.

[4] P. Erdős, On a lemma of Littlewood and Offord, Bull. Amer. Math. Soc. (2nd ser.) 51 (1945), 898-902.

[5] P. Erdős, Problems and results in graph theory and combinatorial analysis, Proc. of the Fifth British Comb. Conf. 1975 Aberdeen, 169-192. Congressus Numerantium, No. XV, Utilitas Math., Winnipeg, Man., 1976.

[6] P. Erdős, C. Ko and R. Rado, Intersection theorems for systems of finite sets, Quart. J. Math. Oxford Ser. 2, 12 (1961) 313-320.

[7] P. Frankl, Extremal set systems, in: R.L. Graham, M. Grötschel, L. Lovász (Eds.), *Handbook of Combinatorics*, Vol. 1, 2, 1293-1329, Elsevier, Amsterdam, 1995.

[8] P. Frankl and Z. Füredi, Forbidding just one intersection, J. Combin. Theory Ser. A 39 (1985), no. 2, 160-176.

[9] P. Frankl and V. Rödl, Forbidden intersections, Trans. Amer. Math. Soc. 300 (1987), 259-286.

[10] P. Frankl and R.M. Wilson, Intersection theorems with geometric consequences, Combinatorica, 1 (1981), 313-368.

[11] G. Katona, Intersection theorems for systems of finite sets, Acta Math. Acad. Sci. Hungar 15 (1964), 329-337.

[12] P. Keevash and B. Sudakov, On a restricted cross-intersection problem, J. Combinatorial Theory Ser. A, 113 (2006), 1536-1542.

[13] J. Littlewood and C. Offord, On the number of real roots of a random algebraic equation III, Mat. Sbornik 12 (1943), 277-285.

[14] D. Lubell, A short proof of Sperner's theorem, Journal of Combinatorial Theory 1 (1966), 299.

[15] D.K. Ray-Chaudhuri and R.M. Wilson. On t-designs, Osaka J. Math., 12 (1975), 737-744.

[16] H. Robbins, A remark on Stirling's formula, Amer. Math. Monthly 62, (1955), 26-29.

[17] J. Sgall, Bounds on pairs of families with restricted intersections, Combinatorica 19 (1999), 555-566.

[18] E. Sperner, Ein Satz über Untermengen einer endlichen Menge, Math. Z. 27, 544-548, 1928.