THEORY OF COMPUTING, Volume 15 (20), 2019, pp. 1–29
www.theoryofcomputing.org

Subsets of Cayley Graphs That Induce Many Edges

Timothy Gowers* Oliver Janzer†

Received October 24, 2018; Revised October 6, 2019; Published December 22, 2019

Abstract: Let G be a regular graph of degree d and let $A \subset V(G)$. Say that A is η*-closed* if the average degree of the subgraph induced by A is at least ηd. This says that if we choose a random vertex $x \in A$ and a random neighbour y of x, then the probability that $y \in A$ is at least η. This paper was motivated by an attempt to obtain a qualitative description of closed subsets of the Cayley graph Γ whose vertex set is $\mathbb{F}_2^{n_1} \otimes \cdots \otimes \mathbb{F}_2^{n_d}$ with two vertices joined by an edge if their difference is of the form $u_1 \otimes \cdots \otimes u_d$. For the matrix case (that is, when $d = 2$), such a description was obtained by Khot, Minzer and Safra, a breakthrough that completed the proof of the 2-to-2 conjecture. In this paper, we formulate a conjecture for higher dimensions, and prove it in an important special case. Also, we identify a statement about η-closed sets in Cayley graphs on arbitrary finite Abelian groups that implies the conjecture and can be considered as a "highly asymmetric Balog–Szemerédi–Gowers theorem" when it holds. We conclude the paper by showing that this statement is not true for an arbitrary Cayley graph. It remains to decide whether the statement can be proved for the Cayley graph Γ.

ACM Classification: G.2.1

AMS Classification: 68R05, 15A69

Key words and phrases: Unique Games Conjecture, tensors, Cayley graphs

*Supported by a Royal Society 2010 Anniversary Research Professorship. He also held a Research Chair of the Fondation Sciences Mathématiques de Paris while this research was carried out.

†Supported by the Fondation Sciences Mathématiques de Paris while part of this research was carried out.

 DOI: 10.4086/toc.2019.v015a020

1 Introduction

The Unique Games Conjecture, formulated by Khot [6] in 2002, is a central conjecture in theoretical computer science. If true, it implies that for a wide class of natural problems it is NP-hard to find even a very crude approximate solution in polynomial time. Recently, a weakening of the conjecture known as the 2-to-2 Games Conjecture, where the approximation is required to be less crude (so it is easier to prove hardness) was proved by Khot, Minzer and Safra [7], a result that is considered as a major step towards the Unique Games Conjecture itself. More precisely, after work by various authors, the problem had been reduced to a statement about a certain Cayley graph, and Khot, Minzer and Safra proved that statement.

The Cayley graph Γ in question has as its vertex set the set of all $m \times n$ matrices over $\mathbb{F}_2$, with two vertices joined by an edge if their difference has rank 1. Let us say that a subset $\mathcal{A} \subset \mathrm{M}_{m,n}(\mathbb{F}_2)$ is η*-closed* if the probability that $A+B \in \mathcal{A}$, when A is chosen uniformly from $\mathcal{A}$ and B is chosen uniformly from all rank-1 matrices, is at least η. In graph terms, this is the probability that a random neighbour of a random point in $\mathcal{A}$ is itself in $\mathcal{A}$.

A simple example of an η-closed set is the set $\{A \in \mathrm{M}_{m,n}(\mathbb{F}_2) : Ax = y\}$, for some pair of vectors $x \in \mathbb{F}_2^n, y \in \mathbb{F}_2^m$. Indeed, if $Ax = y$ and B is a random matrix of rank 1, then $x \in \ker B$ with probability roughly 1/2. But if $x \in \ker B$, then $(A+B)x = y$, so $A+B \in \mathcal{A}$ as well. A very similar, but distinct, example is the set $\{A \in \mathrm{M}_{m,n}(\mathbb{F}_2) : A^T x = y\}$. Let us call sets of one of these two kinds *basic sets*.

We can form further examples by taking intersections of a small number of basic sets. For example, if $x_1, \dots, x_k$ are linearly independent and we take a set of the form

$$\{A \in \mathrm{M}_{m,n}(\mathbb{F}_2) : Ax_1 = y_1, \dots, Ax_k = y_k\},$$

then with probability approximately 2^{-k} each x_i belongs to $\ker B$, so for any A in the set, $A+B$ belongs to the set with probability approximately 2^{-k}. The result of Khot, Minzer and Safra is the following.

Theorem 1.1. *For every $\eta > 0$ there exist $\delta > 0$ and a positive integer k such that if $\mathcal{A}$ is any η-closed subset of $\mathrm{M}_{m,n}(\mathbb{F}_2)$, then there exists an intersection $\mathcal{C}$ of at most k basic sets such that $|\mathcal{A} \cap \mathcal{C}| \geq \delta|\mathcal{C}|$ and $\mathcal{C} \neq \emptyset$.*

In other words, every closed set is dense inside some intersection of a small number of basic sets.

It is well known and not hard to see that this in fact leads to a characterization (at least qualitatively) of closed sets. Indeed, observe first that if $\mathcal{A}$ is η-closed, then the subgraph induced by $\mathcal{A}$ has average degree at least $\eta|\mathcal{B}|$, where $\mathcal{B}$ is the set of rank-1 matrices, and maximal degree at most $|\mathcal{B}|$. Therefore, any subset of $\mathcal{A}$ of size at least $(1-\eta/4)|\mathcal{A}|$ has average degree at least $\eta|\mathcal{B}|/2$. It follows from this observation and Theorem 1.1 that we can find disjoint subsets $\mathcal{A}_1, \dots, \mathcal{A}_r$ of $\mathcal{A}$, subsets $\mathcal{C}_1, \dots, \mathcal{C}_r$ of $\mathrm{M}_{m,n}(\mathbb{F}_2)$, a positive real number $\delta = \delta(\eta)$ and a positive integer $k = k(\eta)$ with the following properties.

1. The sets $\mathcal{A}_i$ are disjoint.

2. Each $\mathcal{C}_i$ is an intersection of at most k basic sets.

3. For each i, $|\mathcal{A}_i \cap \mathcal{C}_i| \geq \delta|\mathcal{C}_i|$.

4. $|\bigcup_i \mathcal{A}_i| \geq \eta|\mathcal{A}|/4$.

Conversely, if such sets exist, then the probability that a random matrix $A \in \mathcal{A}$ belongs to some $\mathcal{A}_i$ is at least $\eta/4$. If it belongs to $\mathcal{A}_i$, then we can use the following lemma. We write $u \otimes v$ for the rank-1 matrix M with $M_{ij} = u_i v_j$, which sends a vector x to the vector $\langle x, v\rangle u$. Note also that $(u \otimes v)^T$ sends x to $\langle x, u\rangle v$.

Lemma 1.2. *Let $\mathcal{C}$ be an intersection of at most k basic sets and let $\mathcal{A} \subset \mathcal{C}$ be a subset of relative density at least δ. Then $\mathcal{A}$ is $2^{-k}(\delta - 2^{-(m-k)})$-closed.*

Proof. Let us set $\mathcal{C}(x,y) = \{A \in \mathrm{M}_{m,n}(\mathbb{F}_2) : Ax = y\}$, and $\mathcal{C}'(x,y) = \{A \in \mathrm{M}_{m,n}(\mathbb{F}_2) : A^T x = y\}$. Let $x_1, \dots, x_k, y_1, \dots, y_k$ be non-zero vectors such that

$$\mathcal{C} = \bigcap_{i=1}^{r} \mathcal{C}(x_i, y_i) \cap \bigcap_{i=r+1}^{k} \mathcal{C}'(x_i, y_i).$$

Let $u \otimes v$ be a rank-1 matrix. If there exists $i \le r$ such that $\langle x_i, v\rangle \ne 0$, then $(A + u \otimes v)(x_i) = y_i + u$, so $A + u \otimes v \notin \mathcal{C}(x_i, y_i)$ and hence $A + u \otimes v \notin \mathcal{C}$. Similarly, if there exists $i > r$ such that $\langle x_i, u\rangle \ne 0$, then $(A + u \otimes v)^T(x_i) = y_i + v$ and again $A + u \otimes v \notin \mathcal{C}$.

We shall now bound from below the probability that $A + u \otimes v \in \mathcal{A}$ given that $A \in \mathcal{A}$ and that $\langle x_i, v\rangle = 0$ for every $i \le r$ and $\langle x_i, u\rangle = 0$ for every $r < i \le k$, noting that the condition on $u \otimes v$ states that $(u,v) \in U \times V$ for a pair of subspaces U and V with codimensions that add up to at most k, a condition that occurs with probability 2^{-k}.

Let us now condition further on the choice of $v \in V$. That means that we fix v, choose a random $u \in U$, and add $u \otimes v$ to A. If we allow u to take the value 0, then the resulting matrix is uniformly distributed in the affine subspace $A + U \otimes v$, so the probability that it is in $\mathcal{A}$ is equal to the relative density of $\mathcal{A}$ inside this affine subspace.

The translates of $U \otimes v$ by matrices in $\mathcal{C}$ partition $\mathcal{C}$. Let us write them as $\mathcal{W}_1, \dots, \mathcal{W}_s$, and let the relative density of $\mathcal{A}$ inside $\mathcal{W}_i$ be δ_i. Then, still fixing v, we have that

$$\mathbb{P}[A + u \otimes v \in \mathcal{A}] = \sum_i \mathbb{P}[A \in \mathcal{W}_i]\, \mathbb{P}[A + u \otimes v \in \mathcal{A} \mid A \in \mathcal{W}_i] = \sum_i \frac{\delta_i^2}{s\delta} \ge \delta.$$

This statement is true regardless of v, so we deduce that the probability that $A + u \otimes v \in \mathcal{A}$ given that $A \in \mathcal{A}$ and $(u,v) \in U \times (V \setminus \{0\})$ is at least δ. If we now insist that $u \ne 0$, we reduce this probability by at most $2^{-(m-k)}$, so the result is proved. □

Let $B \in \mathcal{B}$ be chosen uniformly at random. Given the lemma above, applied to the sets $\mathcal{A}_i$ and $\mathcal{C}_i$, we deduce that the conditional probability that $A + B \in \mathcal{A}_i$ given that $A \in \mathcal{A}_i$ is at least some $c(\delta, k) > 0$, and from that it follows that $\mathcal{A}$ is $c(\delta, k)\eta/4$-closed.

Thus, a set $\mathcal{A}$ is η-closed for some not too small η if and only if an appreciable fraction of $\mathcal{A}$ is efficiently covered by disjoint intersections of few basic sets.

Barak, Kothari and Steurer suggest in [1] that establishing a higher-dimensional analogue of Theorem 1.1 may be a useful step toward obtaining a proof of the full Unique Games Conjecture. The main purpose of this paper is to formulate a possible higher-dimensional analogue of Theorem 1.1 (Conjecture 1.4) and prove some partial results towards it. However, we do not claim a reduction of the Unique Games Conjecture to Conjecture 1.4.

We say that $\mathcal{A} \subset \mathbb{F}_2^{n_1} \otimes \cdots \otimes \mathbb{F}_2^{n_d}$ is η-closed if with probability at least η, we have $A + u_1 \otimes \cdots \otimes u_d \in \mathcal{A}$, when $A \in \mathcal{A}$ and vectors $u_i \in \mathbb{F}_2^{n_i} \setminus \{0\}$ are chosen independently and uniformly at random.

Problem 1.3. Give a qualitative description of η-closed sets $\mathcal{A} \subset \mathbb{F}_2^{n_1} \otimes \cdots \otimes \mathbb{F}_2^{n_d}$.

To see that this is indeed a generalization of the problem about matrices considered above, we identify $\mathrm{M}_{m,n}(\mathbb{F}_2)$ with $\mathbb{F}_2^m \otimes \mathbb{F}_2^n$ in the usual way, which leads to a slight reformulation of Theorem 1.1 in terms of tensor products. Note first that under this identification, the set

$$\{M \in \mathrm{M}_{m,n}(\mathbb{F}_2) : Mx_1 = \cdots = Mx_a = M^T y_1 = \cdots = M^T y_b = 0\}$$

becomes the set $H \otimes K$, where $H = \langle y_1, \ldots, y_b \rangle^\perp$ and $K = \langle x_1, \ldots, x_a \rangle^\perp$. It follows that an intersection of at most k basic sets is either empty or a translate of $H \otimes K$ for some pair of subspaces $H \subset \mathbb{F}_2^m, K \subset \mathbb{F}_2^n$ with $\mathrm{codim}(H) + \mathrm{codim}(K) \leq k$.

In the higher-dimensional case, there is a richer class of sets $\mathcal{A} \subset \mathbb{F}_2^{n_1} \otimes \cdots \otimes \mathbb{F}_2^{n_d}$ that are η-closed. To describe them, we introduce the following piece of notation, which we shall use repeatedly in the rest of the paper. Given a non-empty subset $I \subset [d]$, write $\mathbb{F}_2^I$ for $\bigotimes_{i \in I} \mathbb{F}_2^{n_i}$, so that we naturally have $\mathbb{F}_2^{n_1} \otimes \cdots \otimes \mathbb{F}_2^{n_d} = \mathbb{F}_2^I \otimes \mathbb{F}_2^{I^c}$. Here and elsewhere in the paper, I^c stands for $[d] \setminus I$.

Now we say that $\mathcal{C}$ is *k-simple* if there exists a collection of subspaces $H_I \subset \mathbb{F}_2^I$ of codimension at most k, one for each non-empty subset $I \subset [d]$, such that $\mathcal{C}$ is a translate of the set

$$\bigcap_{I \subset [d], I \neq \emptyset} (H_I \otimes \mathbb{F}_2^{I^c})$$

(where $H_{[d]} \otimes \mathbb{F}_2^{\emptyset}$ is just $H_{[d]}$), which is a subspace of $\mathbb{F}_2^{n_1} \otimes \cdots \otimes \mathbb{F}_2^{n_d}$. It is not hard to see that this subspace contains at least a proportion $c(d,k) > 0$ of all rank-1 tensors $u_1 \otimes \cdots \otimes u_d$ (provided that $n_1, \ldots, n_d$ are sufficiently large), so it is $c(d,k)$-closed. It follows that any translate of it is $c(d,k)$-closed too.

We now make the following conjecture.

Conjecture 1.4. *For any $\eta > 0$ and any positive integer d, there exist $k = k(d,\eta)$ and $\rho = \rho(d,\eta) > 0$ with the following property. Let $\mathcal{A} \subset \mathbb{F}_2^{n_1} \otimes \cdots \otimes \mathbb{F}_2^{n_d}$ be η-closed. Then there is a k-simple set $\mathcal{C}$ such that $|\mathcal{A} \cap \mathcal{C}| \geq \rho |\mathcal{C}|$.*

Note that in the $d = 2$ case, we allow translates of sets $(H_{\{1\}} \otimes H_{\{2\}}) \cap H_{\{1,2\}}$ rather than just translates of $H_{\{1\}} \otimes H_{\{2\}}$, so Conjecture 1.4 might seem to be weaker than Theorem 1.1. However, this actually makes no difference, since when intersecting with $H_{\{1,2\}}$, the cardinality of the set drops by a factor at most 2^k.

The main result of this paper, stated later in this section, is a proof of Conjecture 1.4 in an important special case.

1.1 What can be said about more general Cayley graphs?

It is tempting to try to prove Conjecture 1.4 by identifying and proving a statement that applies to a much wider class of Cayley graphs, of which Conjecture 1.4 would be a special case. We would begin with an Abelian (or even non-Abelian) group G and a pair of subsets $A, B \subset G$, where we think of B as the set of generators, satisfying the hypothesis that $|\{(a,b) \in A \times B : a + b \in A\}| \geq \eta |A||B|$. We shall say in this situation that A is *(B,η)-closed* (in G).

Another way of writing the condition is

$$\langle \mathbb{1}_A * \mu_B, \mathbb{1}_A \rangle \geq \eta \alpha,$$

where α is the density of A, μ_B is the characteristic measure of B (that is, the function that takes the value $|G|/|B|$ on B and 0 elsewhere) and we define $f * g(x)$ to be $\mathbb{E}_{y+z=x} f(y)g(z)$. By the Cauchy-Schwarz inequality the left-hand side is at most $\|\mathbb{1}_A * \mu_B\|_2 \|\mathbb{1}_A\|_2 = \|\mathbb{1}_A * \mu_B\|_2 \alpha^{1/2}$, where inner products and L_p norms are defined using expectations, so our hypothesis implies that $\|\mathbb{1}_A * \mu_B\|_2^2 \geq \eta^2 \alpha$. It is easy to see that this "mixed energy" $\|\mathbb{1}_A * \mu_B\|_2^2$ can be at most α, with equality if and only if $a + b - b' \in A$ for every $a \in A, b, b' \in B$.

At this point let us recall the so-called asymmetric Balog–Szemerédi–Gowers theorem, which can be found in [9] as Theorem 2.35. (For a useful alternative presentation of the theorem, see also [3].) The main assumption of the theorem is that A, B are two finite subsets of an Abelian group, with densities α and β, such that $\|\mathbb{1}_A * \mathbb{1}_B\|_2^2 \geq \eta \alpha \beta^2$ (which is equivalent to saying that $\|\mathbb{1}_A * \mu_B\|_2^2 \geq \eta \alpha$), but there is also an assumption that A is not too much bigger than B. The precise statement is as follows.

Theorem 1.5. *For every $\varepsilon > 0$ there exists a constant $C = C(\varepsilon)$ with the following property. Let G be a finite Abelian group, let $L \geq 1$, let $0 < \eta \leq 1$ and let A and B be finite subsets of G with densities α and β, such that $\alpha \leq L\beta$ and $\|\mathbb{1}_A * \mathbb{1}_B\|_2^2 \geq 2\eta \alpha \beta^2$. Then there exist a subset $H \subset G$ such that $|H + H| \leq C\eta^{-C} L^{\varepsilon} |H|$, a subset $X \subset G$ of size at most $C\eta^{-C} L^{\varepsilon} |A|/|H|$ such that $|A \cap (X + H)| \geq C^{-1} \eta^C L^{-\varepsilon} |A|$, and some $x \in G$ such that $|B \cap (x + H)| \geq C^{-1} \eta^C L^{-\varepsilon} |B|$.*

More qualitatively speaking, if A is not too much larger than B and $\|\mathbb{1}_A * \mathbb{1}_B\|_2^2$ is within a constant of its largest possible value, then there is a set H of small doubling such that a small number of translates of H cover a substantial proportion of A, and some translate of H covers a substantial proportion of B. It is not hard to see that the converse holds as well.

This theorem cannot be used to prove Conjecture 1.4 because of the condition that $\alpha \leq L\beta$, which does not apply here since the set $\mathcal{A}$ in Conjecture 1.4 can be much bigger than the set $\mathcal{B}$. That raises the following question, which generalizes Problem 1.3.

Question 1.6. Let G be a finite Abelian group, let $\eta > 0$, and let $A, B \subset G$ be subsets such that A is (B, η)-closed in G. What can be said about A, B and the relationship between them?

A similar question can of course be asked with the slightly weaker hypothesis that $\|\mathbb{1}_A * \mathbb{1}_B\|_2^2 \geq \eta^2 \alpha \beta^2$, but we shall concentrate on the question as stated, since it is more closely related to Conjecture 1.4.

An immediate observation is that we cannot hope to say anything interesting about the structure of B, even if $\eta = 1$. For example, $\eta = 1$ if $A = G$ and B is an arbitrary subset of G. For a more general example, one can let A be an arbitrary union of cosets of some subgroup H and let B be an arbitrary subset of H. For a slightly different example, let $G = \mathbb{F}_2^n$, let B be the set $\{e_1, \ldots, e_n\}$ of standard basis vectors, and let A be a union of $n/3$-dimensional affine subspaces V_i, such that each V_i is a random translate of the subspace generated by $n/3$ randomly chosen e_j. Then if $x \in V_i$ and $b \in B$, the probability that $x + b \in V_i$ is 1/3, so A is 1/3-closed.

Any general statement will have to be weak enough to allow for examples like these. The last example shows that we cannot hope to find a single set H of small doubling and cover a large portion of A efficiently with translates of H, unless H is of constant size, in which case the conclusion becomes trivial.

To sketch briefly why not, observe first that by Freiman's theorem we can assume that H is a subspace. Next, note that for each vector x, the probability that it belongs to the span of a random $n/3$ standard basis vectors is exponentially small in the size of the support of x. We can also use the following simple lemma.

Lemma 1.7. *Let H be a subspace of dimension d and let $k \le d$. Then the number of vectors in H of support size at most k is at most the number of vectors of support size at most k in the subspace generated by the first d standard basis vectors $e_1, \dots, e_d$, namely $\sum_{i=0}^{k} \binom{d}{i}$.*

Proof. Let $u_1, \dots, u_d$ be a basis for d. By Gaussian elimination, we can convert $u_1, \dots, u_d$ into a basis $v_1, \dots, v_d$ and find coordinates $t_1, \dots, t_d$ such that $v_i(t_j) = \delta_{ij}$. Then the support size of $\sum_i \lambda_i v_i$ is at least the number of non-zero λ_i, which proves the result. □

When d is large, it follows that the proportion of vectors in H of small support is very small. Combining these observations, one can show that for every η there exists d such that if H is a d-dimensional subspace, then the probability that a random subspace V of dimension $n/3$ is $(H, \eta/2)$-closed is at most $\eta/2$. This in turn can be used to prove that with high probability the set A described above (for a suitable number of V_i) is not (H, η)-closed for any H of dimension d or above.

However, these examples do not rule out a weakening along the following lines.

Question 1.8. Let G be a finite Abelian group, let $\eta > 0$, and let A, B be subsets of G such that A is (B, η)-closed in G. Does it follow that A has a non-empty subset A' such that A' is (B, η')-closed in G, and $|A' + A'| \le C|A'|$, where $\eta' > 0$ and C are constants that depend on η only?

An argument similar to the one we mentioned just after the statement of Theorem 1.1 shows that if the answer is yes, then we can find a collection of disjoint subsets $A_1, \dots, A_m$ that cover a substantial proportion of A, each one with small doubling and each one (B, η')-closed (with a slightly smaller η'). Thus, we would be able to obtain a conclusion similar to that of Theorem 1.5 but without the requirement that the structured sets are all translates of one another.

A positive answer would also imply Conjecture 1.4. Indeed, by Freiman's theorem A_i is contained in a subspace V_i not much larger than A_i. This reduces the conjecture to the case where $\mathcal{A}$ is a subspace. In that case, a very simple corollary of our main result, Corollary 1.12 (stated later) proves the conjecture.

However, the answer to Question 1.8 is easily seen to be negative (which implies that it is also negative if we assume the weaker mixed-energy hypothesis instead). The example we are about to give was communicated to us privately by Boaz Barak as a counterexample to a related but slightly different statement.

For convenience let n be odd, let $A \subset \mathbb{F}_2^n$ be the set of all vectors with $(n \pm 1)/2$ coordinates equal to 1, and let B be the set of standard basis vectors. Then it is easy to see that A is (B, η)-closed for $\eta = (n+1)/2n \approx 1/2$. Suppose now that we could find a subset $A' \subset A$ such that $|A' + A'| \le C|A'|$, and A' is (B, η')-closed. By Freiman's theorem, A' is contained in a subspace V that is not much bigger than A', which implies that V is (B, c)-closed for some positive constant $c = c(\eta)$. That implies that at least cn of the standard basis vectors belong to V. Let W be the subspace spanned by these basis vectors. The maximum number of elements of A that can belong to a translate $x + W$ of W is $2(cn)^{-1/2}|W|$, and therefore $|A'| \le 2(cn)^{-1/2}|V|$. This contradicts the fact that V is not much bigger than A'.

In this paper we formulate a yet weaker conjecture and prove that it still implies Conjecture 1.4. Unfortunately, we also give a counterexample to the weaker conjecture. The counterexample does not make the implication vacuous, however, because the implication depends on a non-trivial theorem that is true and of some interest: it is just that for a general Cayley graph (on a finite Abelian group) one cannot deduce the hypotheses of the theorem from the assumption that a set is η-closed. It is conceivable that one might be able to prove Conjecture 1.4 (and thereby also give a different proof of the theorem of Khot, Minzer and Safra) by using additional properties of the particular Cayley graph that that conjecture is about.

How, then, might one try to find a conjecture that would not be contradicted by the "two-layers" example just discussed? One observation that suggests a possible way forward is the following. Suppose that we extend the set by adding a few more layers. If, say, we take not just the middle two layers but the middle ε^{-1} layers (or thereabouts), then we obtain a new set inside which the first set has relative density approximately 2ε, and this new set is $(1-2\varepsilon)$-closed, since a random element of the set will be in one of the interior layers with probability approximately (and in fact slightly bigger than) $1-2\varepsilon$, and adding an arbitrary basis vector to such an element will give another element of the set.

So perhaps we could hope that if A is (B,η)-closed, then there is a set C that is $(B,1-\varepsilon)$-closed such that $|A\cap C|\geq\delta|C|$ for some δ that depends on η and ε only.

However, simple modifications of the example show that this is too much to ask. For instance, we can take as our set A the set of all $x\in\mathbb{F}_2^n$ such that m or $m+1$ coordinates are equal to 1 and all but the first $2m$ coordinates are zero. If m is around $n/4$, say, then the resulting set is $(B,1/4)$-closed, but there is no prospect of A living densely in a set that is almost perfectly closed, because of the need to add basis vectors corresponding to coordinates beyond $2m$.

A further example to consider is the set of all $x\in\mathbb{F}_2^n$ such that at most $n/3$ coordinates are equal to 1. This set is $(B,1/3)$-closed (at least—in fact it is more like $(B,2/3)$-closed because the probability that a random element of the set has exactly $\lfloor n/3\rfloor$ coordinates equal to 1 is approximately $1/2$), but for similar reasons to the previous example, one cannot find an almost perfectly closed set with a significant proportion of its elements in the set.

However, the picture changes if we ask for slightly less. Let us informally call a set C *good* if there is a proportional-sized subset $B'\subset B$ such that C is $(B',1-\varepsilon)$-good for some small constant ε. Thus, now we ask only that C should be almost closed for a *large subset* of B rather than for the whole set.

It is not immediately clear how to use this definition, because the statement that $|A\cap C|\geq\delta|C|$ for a good set C can be true for uninteresting reasons. For example, we could take C to be the union of a subspace V generated by $n/5$ basis vectors together with an arbitrary subset of A of cardinality $2\delta|V|$. To remedy this, we insist that C is "related to A" in the graph in a different sense from that of A being dense in C.

Here, then, is a question that replaces Question 1.8.

Question 1.9. Is it true that for every $\eta,\varepsilon>0$ there exist $c>0,\delta>0$ and positive integer l with the following property? Let G be a finite Abelian group and let $A,B\subset G$ be subsets such that A is (B,η)-closed. Then there is a subset $B'\subset B$ and a non-empty subset $C\subset G$ with the following properties.

1. $|B'|\geq\delta|B|$.
2. C is $(B',1-\varepsilon)$-closed.
3. $C\subset\left\{x\in G:\mathbb{1}_A*\mu_B*\cdots*\mu_B*\mu_{-B}*\cdots*\mu_{-B}(x)\geq c\right\}$ where the number of μ_Bs and μ_{-B}s in the convolution is l.

Condition (3) is saying that for any $x \in C$, the probability that $x - b_1 - \cdots - b_l + b_{l+1} + \cdots + b_{2l} \in A$, when the b_i are chosen uniformly and independently at random from B, is at least c. When the group G is $\mathbb{F}_2^n$ for some n, we can and will simplify it, since $B = -B$.

To see that this question improves on Question 1.8, let us consider the two problematic examples for that question. If m is odd and $A \subset \mathbb{F}_2^n$ consists of all sequences with $(m \pm 1)/2$ 1s and with no 1s after the mth coordinate, then let C be the set of all sequences with no 1s after the mth coordinate that have between $(m-1)/2 - \varepsilon^{-1}$ and $(m+1)/2 + \varepsilon^{-1}$ 1s. If $l = \varepsilon^{-1}$, then for any $x \in C$, the probability that $x - b_1 - \cdots - b_l \in A$ is at least $(m/(2n))^l$. (This is because conditional on $b_i \in \{e_1, \ldots, e_m\}$ this probability is at least $1/2^l$.) Moreover, if $B' = \{e_1, \ldots, e_m\}$, then for every $b \in B'$ and every $c \in C$ that is not on the boundary (in the obvious sense), we have that $b + c \in C$, so C is $(B', 1-\varepsilon)$-closed.

Now let us look at the example where A is the set of all sequences with at most $n/3$ 1s. This time let C be the set of all sequences that are 0 after the first $2n/3$ coordinates and have at most $n/3 + \varepsilon^{-1}$ 1s, and let $B' = \{e_1, \ldots, e_{2n/3}\}$. Then for any $x \in C$, the probability that $x - b_1 - \cdots - b_l \in A$ is at least $(1/3)^l$, where $l = \varepsilon^{-1}$. Moreover, C is $(1-\varepsilon)$-closed, again because adding an element of B' to a non-boundary element of C gives an element of C.

Finally, note that even in the case where G is the group of $n_1 \times n_2$ matrices over $\mathbb{F}_2$ and B is the set of matrices of rank 1, we cannot necessarily take B' to equal B in Question 1.9. Indeed, if $u \in \mathbb{F}_2^{n_2}$ is non-zero and $A = \{M \in G : Mu = 0\}$, then for any $c > 0$ and any l, if n_1 and n_2 are sufficiently large, then $\big\{x \in G : \mathbb{1}_A * \mu_B * \cdots * \mu_B * \mu_{-B} * \cdots * \mu_{-B}(x) \geq c\big\} \subset A$, where the number of μ_Bs and μ_{-B}s in the convolution is l. However, it is easy to see that no subset of A is $(B, 3/4)$-closed.

1.2 Our main result

Let us now see why a positive answer to Question 1.9 would imply Conjecture 1.4. The deduction will be easy once we have established the following theorem, which is the main result of this paper. In the statement of the theorem, and in the rest of this paper, $\mathcal{G}$ denotes $\mathbb{F}_2^{n_1} \otimes \cdots \otimes \mathbb{F}_2^{n_d}$ and $\mathcal{B}$ denotes the multiset $\{u_1 \otimes \cdots \otimes u_d : u_i \in \mathbb{F}_2^{n_i} \text{ for all } i\}$ (which is a multiset only because some of the u_i can be zero). Note that the notion of (B, η)-closedness can be generalized in an obvious way to multisets.

Theorem 1.10. *For any $\theta > 0$, there exists $\varepsilon = \varepsilon(d, \theta) > 0$ with the following property. Let $\delta > 0$. Then there exists a positive integer $k = k(d, \delta)$ with the following property. For any $\mathcal{B}' \subset \mathcal{B}$ with $|\mathcal{B}'| \geq \delta|\mathcal{B}|$ and any $\mathcal{A} \subset \mathcal{G}$ which is $(\mathcal{B}', 1-\varepsilon)$-closed, there exists a k-simple set $\mathcal{D} \subset \mathcal{G}$ such that $|\mathcal{D} \cap \mathcal{A}| \geq (1-\theta)|\mathcal{D}|$.*

We remark that in the case where $\mathcal{B}' = \mathcal{B}$ the proof is easy, and $\mathcal{D}$ can be chosen to be the whole of $\mathcal{G}$.

It is convenient to state the following corollary separately, which follows from Theorem 1.10 by taking $\theta = 1/2$.

Corollary 1.11. *There exists $\varepsilon = \varepsilon(d) > 0$ such that for any $\delta > 0$, there exists a positive integer $k = k(d, \delta)$ with the following property. For any $\mathcal{B}' \subset \mathcal{B}$ with $|\mathcal{B}'| \geq \delta|\mathcal{B}|$ and any $\mathcal{A} \subset \mathcal{G}$ which is $(\mathcal{B}', 1-\varepsilon)$-closed, there exists a k-simple set $\mathcal{D} \subset \mathcal{G}$ which has $|\mathcal{D} \cap \mathcal{A}| \geq (1/2)|\mathcal{D}|$.*

Let us see why Conjecture 1.4 follows from Corollary 1.11 and a positive answer to Question 1.9 in the case of the group $\mathcal{G}$ and the subset $B \subset \mathcal{G}$ of rank-1 tensors. Let $\eta > 0$. Pick $\varepsilon = \varepsilon(d)$ so that the conclusion of Corollary 1.11 holds. If the answer to Question 1.9 is positive for $\mathcal{G}$ and B, then we can choose $c > 0, \delta > 0$, and a positive integer l such that the conclusion of the question is true. Now let $\mathcal{A} \subset \mathcal{G}$ be η-closed. This is saying that $\mathcal{A}$ is (B,η)-closed. By the conclusion of Question 1.9, there exist a set $B' \subset B$ with $|B'| \geq \delta|B|$, and a non-empty subset $\mathcal{C} \subset \mathcal{G}$ such that $\mathcal{C}$ is $(B', 1-\varepsilon)$-closed and $\mathcal{C} \subset \left\{x \in \mathcal{G} : \mathbb{1}_{\mathcal{A}} * \mu_B * \cdots * \mu_B(x) \geq c\right\}$, where the number of μ_Bs in the convolution is l. Define $\mathcal{B}'$ to be the multiset that consists of the set B' together with the multiset of all $u_1 \otimes \cdots \otimes u_d$ with $u_i \in \mathbb{F}_2^{n_i}$ for each i and with at least one u_i equal to 0. Note that $|\mathcal{B}'| \geq \delta|\mathcal{B}|$ and $\mathcal{C}$ is $(\mathcal{B}', 1-\varepsilon)$-closed. By Corollary 1.11, there exists a k-simple set $\mathcal{D} \subset \mathcal{G}$, for some $k = k(d,\delta)$, which has $|\mathcal{D} \cap \mathcal{C}| \geq (1/2)|\mathcal{D}|$. Now pick $x \in \mathcal{D}$ and $b_1, \ldots, b_l \in B$ uniformly and independently at random. The probability that $x - b_1 - \cdots - b_l \in \mathcal{A}$ is at least $c/2$. Therefore, there exists some $y \in \mathcal{G}$ such that when $x \in \mathcal{D}$ is randomly chosen, the probability that $x - y \in \mathcal{A}$ is at least $c/2$. That is,

$$|(\mathcal{D} - y) \cap \mathcal{A}| \geq \frac{1}{2}c|\mathcal{D}| = \frac{1}{2}c|\mathcal{D} - y|.$$

But $\mathcal{D} - y$ is a k-simple set, which finishes the proof of Conjecture 1.4.

Another simple corollary of Theorem 1.10 is the following result, which is Conjecture 1.4 in the case where $\mathcal{A}$ is a subspace.

Corollary 1.12. *For any $\eta > 0$ and any positive integer d, there exists some $k = k(d,\eta)$ with the following property. If $V \subset \mathcal{G}$ is a subspace which is η-closed, then V contains a k-simple subspace. That is,*

$$V \supset \bigcap_{I \subset [d], I \neq \emptyset} (H_I \otimes \mathbb{F}_2^{I^c})$$

for some collection of subspaces $H_I \subset \mathbb{F}_2^I$ of codimension at most k.

Proof. Since V is a vector space, the condition that V is η-closed says that $u_1 \otimes \cdots \otimes u_d \in V$ for at least a proportion of η of all rank-1 tensors $u_1 \otimes \cdots \otimes u_d$. Thus, there exists some $\mathcal{B}' \subset \mathcal{B}$ with $|\mathcal{B}'| \geq \eta|\mathcal{B}|$ such that V is $(\mathcal{B}', 1)$-closed. Taking θ sufficiently close to 0 in Theorem 1.10, it follows that $V \supset \mathcal{D}$ for a k-simple set $\mathcal{D}$, where k depends only on d and η. Then $\mathcal{D}$ is a translate of

$$\bigcap_{I \subset [d], I \neq \emptyset} (H_I \otimes \mathbb{F}_2^{I^c})$$

for some $H_I \subset \mathbb{F}_2^I$ of codimension at most k. Since V is a vector space, it follows that

$$V \supset \bigcap_{I \subset [d], I \neq \emptyset} (H_I \otimes \mathbb{F}_2^{I^c}). \qquad \square$$

In the next section, we shall prove Theorem 1.10. In the last section, we show that the answer to Question 1.9 is negative.

2 The proof of Theorem 1.10

Note that $\mathcal{G} = \mathbb{F}_2^{n_1} \otimes \cdots \otimes \mathbb{F}_2^{n_d}$ can be viewed as the set of d-dimensional $(n_1, \ldots, n_d)$-arrays over $\mathbb{F}_2$ which in turn can be viewed as $\mathbb{F}_2^{n_1 n_2 \ldots n_d}$, equipped with the entry-wise dot product.

The proof of Theorem 1.10 will be reasonably simple once we have established the following result. In the statement of this lemma, and in the rest of this section, we write kB to mean the set of elements of $\mathcal{G}$ that can be written as a sum of *at most* k elements of B, where B is some fixed (multi)subset of $\mathcal{G}$.

Lemma 2.1. *For all $\delta > 0$ and $d \in \mathbb{N}$ there exist $f_1(d), f_3(d) > 0$ and $f_2(d,\delta) \in \mathbb{N}$ with the following property. Let $\mathcal{B}' \subset \mathcal{B}$ be a multiset such that $|\mathcal{B}'| \geq \delta|\mathcal{B}|$. Then there exists a multiset Q whose elements are chosen from $f_1(d)\mathcal{B}'$ (but with arbitrary multiplicity) with the following property. The set of arrays $r \in \mathcal{G}$ with $r.q = 0$ for at least $(1 - f_3(d))|Q|$ choices $q \in Q$ is contained in*

$$\sum_{I\subset[d], I\neq\emptyset} V_I \otimes \mathbb{F}_2^{I^c}$$

for a collection of subspaces $V_I \subset \mathbb{F}_2^I$ that each have dimension at most $f_2(d,\delta)$.

In order to deduce Theorem 1.10 from this lemma, we shall use Fourier analysis. Recall that if A is a subset of $\mathcal{G}$ of density α, then by Parseval's identity we have $\alpha = \sum_r |\widehat{\mathbb{1}_A}(r)|^2$. Also, if B is a multiset in $\mathcal{G}$, then by Parseval's identity and the convolution law, $\langle \mathbb{1}_A * \mu_B, \mathbb{1}_A\rangle = \sum_r |\widehat{\mathbb{1}_A}(r)|^2 \widehat{\mu}_B(r)$ (for a multiset B, we define $\mu_B(x) = (|G|/|B|)B(x)$ where $B(x)$ is the multiplicity of x in B). Thus, the condition that A is (B,η)-closed can be rewritten as the inequality

$$\sum_r |\widehat{\mathbb{1}_A}(r)|^2 \widehat{\mu}_B(r) \geq \eta \sum_r |\widehat{\mathbb{1}_A}(r)|^2.$$

Another fact we shall use later is that if W is a subspace of $\mathcal{G}$, then $\widehat{\mu_W}(r)$ equals $\mathbb{E}_{w\in W}(-1)^{r.w}$, which is 1 if r belongs to the orthogonal complement of W and 0 otherwise.

Lemma 2.2. *Let G be an Abelian group, let $A \subset G$ be a finite subset, let $\eta_1, \eta_2 > 0$, and let $b_1, b_2 \in G$. Suppose that A is $(\{b_1\}, 1-\eta_1)$-closed and $(\{b_2\}, 1-\eta_2)$-closed in G. Then A is $(\{b_1+b_2\}, 1-\eta_1-\eta_2)$-closed in G.*

Proof. Let $A_{\text{bad}} = \{a \in A : a + b_2 \notin A\}$. Then $|A_{\text{bad}}| \leq \eta_2|A|$, by hypothesis. So when $a \in A$ is chosen randomly, we have that

$$\mathbb{P}[a+b_1+b_2 \notin A] \leq \mathbb{P}[a+b_1 \notin A] + \mathbb{P}[a+b_1 \in A_{\text{bad}}] \leq \eta_1 + \eta_2.$$

The result follows. □

We are now in a position to deduce Theorem 1.10 from Lemma 2.1. In the proof, and in the rest of this section, whenever a new function g_i appears, we mean that there exists a function g_i with the claimed property.

Proof of Theorem 1.10. Let $\theta, \delta > 0$, $\mathcal{B}' \subset \mathcal{B}$ with $|\mathcal{B}'| \geq \delta|\mathcal{B}|$, and suppose that $\mathcal{A} \subset \mathcal{G}$ is $(\mathcal{B}', 1-\varepsilon)$-closed, where ε is to be specified. Let $\mathcal{B}'' = \{b \in \mathcal{B}' : \mathcal{A} \text{ is } (\{b\}, 1-2\varepsilon)\text{-closed}\}$. Clearly, $|\mathcal{B}''| \geq (1/2)|\mathcal{B}'|$. Using Lemma 2.1, we can find a multiset Q with elements chosen from $g_1(d)\mathcal{B}''$ such that the set of arrays $r \in \mathcal{G}$ with $r.q = 0$ for at least $(1-g_2(d))|Q|$ choices $q \in Q$ (where $g_2(d) > 0$) is contained in

$$\sum_{I\subset[d], I\neq\emptyset} V_I \otimes \mathbb{F}_2^{I^c}$$

for subspaces $V_I \subset \mathbb{F}_2^I$ of dimension at most $g_3(d,\delta)$. Then, by Lemma 2.2, $\mathcal{A}$ is $(\{b\}, 1-2g_1(d)\varepsilon)$-closed for every $b \in Q$, since each such b is an element of $g_1(d)\mathcal{B}''$. In particular, $\mathcal{A}$ is $(Q, 1-2g_1(d)\varepsilon)$-closed, and therefore

$$\sum_r |\widehat{\mathbb{1}_{\mathcal{A}}}(r)|^2 \widehat{\mu}_Q(r) \geq (1-2g_1(d)\varepsilon) \sum_r |\widehat{\mathbb{1}_{\mathcal{A}}}(r)|^2.$$

By Markov's inequality, it follows that

$$\sum_{r: \widehat{\mu}_Q(r) < 1-2g_2(d)} |\widehat{\mathbb{1}_{\mathcal{A}}}(r)|^2 \leq \frac{g_1(d)\varepsilon}{g_2(d)} \sum_r |\widehat{\mathbb{1}_{\mathcal{A}}}(r)|^2.$$

Choosing $\varepsilon = \varepsilon(d,\theta) > 0$ to be at most $\theta g_2(d)/g_1(d)$, we therefore have

$$\sum_{r: \widehat{\mu}_Q(r) \geq 1-2g_2(d)} |\widehat{\mathbb{1}_{\mathcal{A}}}(r)|^2 \geq (1-\theta) \sum_r |\widehat{\mathbb{1}_{\mathcal{A}}}(r)|^2.$$

Now if $\widehat{\mu}_Q(r) \geq 1-2g_2(d)$ then $r.q = 0$ for at least $(1-g_2(d))|Q|$ choices $q \in Q$. Thus, we have

$$\sum_{r \in T} |\widehat{\mathbb{1}_{\mathcal{A}}}(r)|^2 \geq (1-\theta) \sum_{r \in \mathcal{G}} |\widehat{\mathbb{1}_{\mathcal{A}}}(r)|^2 \tag{2.1}$$

where $T = \sum_{I \subset [d], I \neq \emptyset} V_I \otimes \mathbb{F}_2^{I^c}$. Let

$$R = T^\perp = \bigcap_{I \subset [d], I \neq \emptyset} V_I^\perp \otimes \mathbb{F}_2^{I^c}.$$

Because $\widehat{\mu_R}$ is the characteristic function of T, (2.1) is equivalent to the inequality

$$\sum_{r \in \mathcal{G}} |\widehat{\mathbb{1}_{\mathcal{A}}}(r)|^2 \widehat{\mu_R}(r) \geq (1-\theta) \sum_{r \in \mathcal{G}} |\widehat{\mathbb{1}_{\mathcal{A}}}(r)|^2,$$

which in physical space is the inequality

$$\langle \mathbb{1}_{\mathcal{A}} * \mathbb{1}_{\mathcal{A}}, \mu_R \rangle \geq (1-\theta)\|\mathbb{1}_{\mathcal{A}}\|_2^2 = (1-\theta)\alpha,$$

where α is the density of $\mathcal{A}$. Equivalently,

$$\langle \mu_{\mathcal{A}} * \mu_R, \mathbb{1}_{\mathcal{A}} \rangle \geq 1-\theta,$$

which tells us that if a random element of $\mathcal{A}$ is added to a random element of R, then the sum belongs to $\mathcal{A}$ with probability at least $1-\theta$. The number of triples $(a_1,a_2,r) \in \mathcal{A} \times \mathcal{A} \times R$ with $a_1+a_2 = r$ is therefore at least $(1-\theta)|\mathcal{A}||R|$, and therefore, by averaging, there exists $a \in \mathcal{A}$ such that $|(R-a) \cap \mathcal{A}| \geq (1-\theta)|R| = (1-\theta)|R-a|$. But $R-a$ is $g_3(d,\delta)$-simple, so we can take $k = g_3(d,\delta)$ and $\mathcal{D} = R-a$. □

It remains to prove Lemma 2.1.

2.1 The proof of Lemma 2.1 in the matrix case

For the reader's convenience, in this subsection we give the proof of Lemma 2.1 in the matrix case: that is, the case when $d = 2$. Accordingly, in this subsection, $\mathcal{G}$ will be the group $\mathbb{F}_2^{n_1} \otimes \mathbb{F}_2^{n_2}$ and $\mathcal{B}$ will be the multiset that consists of all rank-1 matrices $u_1 \otimes u_2$ with $u_1 \in \mathbb{F}_2^{n_1}$ and $u_2 \in \mathbb{F}_2^{n_2}$, with multiplicity. (As already remarked, the non-trivial multiplicity comes from when u_1 or u_2 is zero.)

Lemma 2.3. *Let $\mathcal{B}' \subset \mathcal{B}$ be such that $|\mathcal{B}'| \geq \delta|\mathcal{B}|$. Then there exist k depending only on δ, a subspace $U \subset \mathbb{F}_2^{n_1}$, and a subspace $V_u \subset \mathbb{F}_2^{n_2}$ for each $u \in U$, such that all these subspaces have codimension at most k, and such that every $u \otimes v$ with $u \in U, v \in V_u$ belongs to $16\mathcal{B}'$. Moreover, we can insist that all V_u have the same codimension.*

Proof. For each $u \in \mathbb{F}_2^{n_1}$, let

$$\mathcal{B}'_u = \{v \in \mathbb{F}_2^{n_2} : u \otimes v \in \mathcal{B}'\} \quad \text{and let} \quad T = \{u \in \mathbb{F}_2^{n_1} : |\mathcal{B}'_u| \geq (\delta/2)2^{n_2}\}.$$

By averaging, we have that $|T| \geq (\delta/2)2^{n_1}$.

If $u \in T$, then $\mathcal{B}'_u$ has density at least $\delta/2$ in $\mathbb{F}_2^{n_2}$, so by Bogolyubov's lemma (see for example Proposition 4.39 of [9]) $4\mathcal{B}'_u = 2\mathcal{B}'_u - 2\mathcal{B}'_u$ contains a subspace W_u of codimension at most $k_1 = k_1(\delta)$. By Bogolyubov's lemma again, there is a subspace U of codimension at most k_1 contained in $4T$. Let $u \in U$. Then pick $t_1, t_2, t_3, t_4 \in T$ arbitrarily such that $u = t_1 + t_2 + t_3 + t_4$ and set $V_u = \bigcap_{i=1}^4 W_{t_i}$. Note that V_u has codimension at most $4k_1$ for every $u \in U$. If $v \in V_u$, then $t_i \otimes v \in 4\mathcal{B}'$ for $i = 1, \dots, 4$, therefore $u \otimes v \in 16\mathcal{B}'$. Thus, we can take $k = 4k_1$.

For the last assertion, note that we may replace V_u with any subspace of it, and we still have $u \otimes V_u \subset 16\mathcal{B}'$. □

In the next three lemmas k is a positive integer, U is a subspace of $\mathbb{F}_2^{n_1}$ and for each $u \in U$, V_u is a subspace of $\mathbb{F}_2^{n_2}$ such that all these subspaces have codimension at most k and all the V_u have the same codimension. We take $Q = \bigcup_{u \in U}(u \otimes V_u)$ and prove that this choice is suitable for Lemma 2.1.

Lemma 2.4. *There exists an absolute constant $\varepsilon > 0$ with the following property. The set of arrays $r \in \mathcal{G}$ with $r.q = 0$ for at least $(1-\varepsilon)|Q|$ choices $q \in Q$ is contained in $W_{12} + W_1 \otimes \mathbb{F}_2^{n_2} + \mathbb{F}_2^{n_1} \otimes W_2$ where $W_{12} \subset \mathbb{F}_2^{n_1} \otimes \mathbb{F}_2^{n_2}, W_1 \subset \mathbb{F}_2^{n_1}$ and $W_2 \subset \mathbb{F}_2^{n_2}$ are subspaces of dimension at most $f(k)$.*

Before we prove this lemma, we need to establish the following result. In the statement, and in the rest of this section, we use the following convention for the multiplication of arrays $r \in \mathbb{F}_2^{n_1} \otimes \cdots \otimes \mathbb{F}_2^{n_{a+b}}$ and $s \in \mathbb{F}_2^{n_1} \otimes \cdots \otimes \mathbb{F}_2^{n_a}$. Define $rs \in \mathbb{F}_2^{n_{a+1}} \otimes \cdots \otimes \mathbb{F}_2^{n_{a+b}}$ to be the array with

$$(rs)_{i_{a+1},\dots,i_{a+b}} = \sum_{j_1,\dots,j_a} r_{j_1,\dots,j_a,i_{a+1},\dots,i_{a+b}} s_{j_1,\dots,j_a}.$$

Note that in the case when r is a matrix and s is a vector, this is not quite the same as the standard convention since we sum over the first coordinate of the matrix instead of the second. If r and s are arrays of the same size, then we use the notation $r.s$ for the product of r and s, since then it coincides with the obvious notion of dot product, and it is useful to think of it that way.

Lemma 2.5. *For $m = 2^{k+3}$, let $r_1, \dots, r_m \in \mathcal{G}$ be such that for every $i \le m$ there are at least $(3/4)|Q|$ choices of $q \in Q$ such that $r_i.q = 0$. Then there exist $i \ne j$ such that $(r_i - r_j)w = 0$ for at least $\rho(k)2^{n_1}$ choices $w \in \mathbb{F}_2^{n_1}$, for some positive function $\rho(k)$. Thus, there exist $i \ne j$ such that $r_i - r_j$ has rank at most $l(k)$.*

Proof. For each $i \le m$, there are at least $|U|/2$ choices of $u \in U$ such that $r_i.(u \otimes v) = 0$ for more than $|V_u|/2$ choices of $v \in V_u$. But $r_i.(u \otimes v) = (r_i u).v$, so this implies that $r_i u \in V_u^\perp$.

It follows that for at least $|U|/4$ choices of $u \in U$ we have $r_i u \in V_u^\perp$ for at least $m/4$ choices of $i \le m$. Since $m/4 > |V_u^\perp|$, for every such u there exist $i \ne j$ with $r_i u = r_j u$. Thus, for some $i \ne j$, there are at least $|U|/(4m^2)$ choices of $u \in U$ with $r_i u = r_j u$. The result follows. □

Lemma 2.5 reduces Lemma 2.4 to the following.

Lemma 2.6. *There exists an absolute constant $\varepsilon' > 0$ with the following property. The set of arrays $r \in \mathcal{G}$ of rank at most l such that $r.q = 0$ for at least $(1-\varepsilon')|Q|$ choices $q \in Q$ is contained in $W_1 \otimes \mathbb{F}_2^{n_2} + \mathbb{F}_2^{n_1} \otimes W_2$ where $W_1 \subset \mathbb{F}_2^{n_1}$ and $W_2 \subset \mathbb{F}_2^{n_2}$ are subspaces of codimension at most $f(k,l)$.*

Indeed, take ε' as given by Lemma 2.6 and let $\varepsilon = \min(\varepsilon'/2, 1/4)$. We claim that ε is suitable for Lemma 2.4. Take $l(k)$ as given by Lemma 2.5. Choose a maximal set $x_1, x_2, \dots, x_t \in \mathcal{G}$ with the property that for every $i \le t$, we have $x_i.q = 0$ for at least $(1-\varepsilon)|Q|$ choices $q \in Q$, and for every $1 \le i < j \le t$, $x_i - x_j$ has rank greater than $l(k)$. By Lemma 2.5, $t \le 2^{k+3}$. Now if some $r \in \mathcal{G}$ has $r.q = 0$ for at least $(1-\varepsilon)|Q|$ choices $q \in Q$, then by the maximality of the x_j's it follows that $r - x_i$ has rank at most $l(k)$ for some $i \le t$. Moreover, $(r - x_i).q = 0$ for at least $(1-\varepsilon')|Q|$ choices $q \in Q$, so by Lemma 2.6, $r - x_i$ is contained in $W_1 \otimes \mathbb{F}_2^{n_2} + \mathbb{F}_2^{n_1} \otimes W_2$ where W_1, W_2 have codimension at most $g(k)$ and do not depend on r. So we may take W_{12} to be the span of all the x_i.

Proof of Lemma 2.6. We shall prove that we can take ε' to be $1/8$, W_1 to be $U^\perp$ and W_2 to be a subspace that we define as follows. Let

$$X = \left\{ x \in \mathbb{F}_2^{n_2} : x \in V_u^\perp \text{ for at least } \frac{|U|}{10 \cdot 2^l} \text{ choices } u \in U \right\}.$$

Since $|V_u^\perp| \le 2^k$ for every $u \in U$, we have

$$|X| \le \frac{|U| \cdot 2^k}{|U|/10 \cdot 2^l} = 10 \cdot 2^{k+l}.$$

Let $W_2 = \operatorname{span}(X)$.

Now let r be a matrix of rank at most l such that $r.q = 0$ for at least $7|Q|/8$ choices of $q \in Q$. Then $ru \in V_u^\perp$ for at least $3|U|/4$ choices of $u \in U$. Since r has rank at most l, we have $r \in \mathbb{F}_2^{n_1} \otimes H_2(r)$ for some subspace $H_2(r) \subset \mathbb{F}_2^{n_2}$ with $\dim(H_2(r)) \le l$. By definition, for any $v \notin W_2$, the number of $u \in U$ with $v \in V_u^\perp$ is at most $|U|/(10 \cdot 2^l)$. Since $|H_2(r)| \le 2^l$ and $ru \in H_2(r)$ for every $u \in U$, the number of $u \in U$ with $ru \in V_u^\perp \setminus W_2$ is at most $|U|/10$. It follows that for more than $|U|/2$ choices $u \in U$ we have $ru \in W_2$. This in fact implies that $ru \in W_2$ for all $u \in U$. Take a basis $y_1, \dots, y_a$ for W_2 and extend it to a basis $y_1, \dots, y_a, y'_1, \dots, y'_b$ for $\mathbb{F}_2^{n_2}$. Choose $x_i, x'_j \in \mathbb{F}_2^{n_1}$ such that

$$r = \sum_{1 \le i \le a} x_i \otimes y_i + \sum_{1 \le j \le b} x'_j \otimes y'_j.$$

For every $u \in U$, we have

$$ru = \sum_{1 \le i \le a} (x_i.u) y_i + \sum_{1 \le j \le b} (x'_j.u) y'_j,$$

so $x'_j.u = 0$ holds for every $1 \le j \le b$ and every $u \in U$. Thus, $r \in \mathbb{F}_2^{n_1} \otimes W_2 + U^{\perp} \otimes \mathbb{F}_2^{n_2}$. □

2.2 The proof of Lemma 2.1 in the general case

It is convenient to introduce a few definitions.

Definition 2.7. Let k be a positive integer and let $\varepsilon > 0$. Let Q be a multiset with elements chosen from $\mathcal{G}$ (with arbitrary multiplicity). We say that Q is (k, α)-*forcing* if the set of all arrays $r \in \mathcal{G}$ with $r.q = 0$ for at least $\alpha |Q|$ choices $q \in Q$ is contained in a set of the form

$$\sum_{I \subset [d], I \neq \emptyset} V_I \otimes \mathbb{F}_2^{I^c}$$

for some choice of subspaces $V_I \subset \mathbb{F}_2^I$ of dimension at most k.

Note that the conclusion of Lemma 2.1 is that the multiset Q is $(f_2(d,\delta), 1 - f_3(d))$-forcing.

Definition 2.8. We say that the hypothesis (H) holds for d if the following is true. For every $\delta > 0$ there exist $f_1(d), f_2(d,\delta)$ and $f_3(d) > 0$ such that if $\mathcal{B}' \subset \mathcal{B}$ is such that $|\mathcal{B}'| \ge \delta |\mathcal{B}|$, then there exists a multiset Q, with elements chosen from $\mathcal{B} \cap f_1(d)\mathcal{B}'$, that is $(f_2(d,\delta), 1 - f_3(d))$-forcing.

Hypothesis (H) is the one that really interests us, since if it holds for every d then Lemma 2.1 is proved. However, in order to get an induction to work we shall need a slight strengthening that says that we can ask for the elements of Q to belong to a large subspace of a suitable form.

Definition 2.9. We say that the hypothesis (H') holds for d if the following is true. For every $\delta > 0$ and every positive integer l there exist $f_1(d), f_2(d,\delta,l)$ and $f_3(d) > 0$ such that if $\mathcal{B}' \subset \mathcal{B}$ is such that $|\mathcal{B}'| \ge \delta |\mathcal{B}|$, and for every non-empty $I \subset [d]$, $L_I \subset \mathbb{F}_2^I$ is a subspace of codimension at most l, then there exists a multiset Q, with elements chosen from

$$\mathcal{B} \cap (f_1(d)\mathcal{B}') \cap \bigcap_I (L_I \otimes \mathbb{F}_2^{I^c}),$$

that is $(f_2(d,\delta,l), 1 - f_3(d))$-forcing.

In what follows, we shall prove that if (H) holds for d, then so does (H'), and that if (H') holds for all $d' < d$, then (H) holds for d. This completes the proof since (H) holds for $d = 1$. Indeed, if $\mathcal{B}' \subset \mathbb{F}_2^{n_1}$ has $|\mathcal{B}'| \ge \delta \cdot 2^{n_1}$, then by Bogolyubov's lemma, $4\mathcal{B}' = 2\mathcal{B}' - 2\mathcal{B}'$ contains a subspace $U \subset \mathbb{F}_2^{n_1}$ of codimension at most $g(\delta)$. If $x.u = 0$ for over half the elements of U, then the set of $u \in U$ with $x.u = 0$ is not contained in a proper subspace, so $x \in U^{\perp}$, which has dimension at most $g(\delta)$. This implies that U is $(g(\delta), 3/4)$-forcing.

The next few results are needed for technical reasons. The set introduced in the next definition behaves well under certain algebraic operations, such as intersecting with a dense subspace. It is a generalization of the set $\bigcup_{u \in U} (u \otimes V_u)$ used in the previous subsection.

Definition 2.10. Suppose that we build a collection of subspaces as follows. We begin with a subspace $U \subset \mathbb{F}_2^{n_1}$. Then for each $u_1 \in U$ we take a subspace $U_{u_1} \subset \mathbb{F}_2^{n_2}$, for each $u_1 \in U$ and $u_2 \in U_{u_1}$ we take a subspace $U_{u_1,u_2} \subset \mathbb{F}_2^{n_3}$, and so on up to subspaces $U_{u_1,\dots,u_{d-1}}$. Now let Q be the multiset that consists of all tensors $u_1 \otimes \cdots \otimes u_d$ such that $u_1 \in U, u_2 \in U_{u_1}, \dots, u_d \in U_{u_1,\dots,u_{d-1}}$. If all the subspaces in the collection have codimension at most l, then we say that Q is an *l-system*.

Lemma 2.11. *Let Q be an l-system and let Q' be a l'-system. Then $Q \cap Q'$ contains an $(l+l')$-system.*

Proof. Let Q have spaces as in Definition 2.10 and let Q' have spaces $U'_{u'_1,\dots,u'_{k-1}}$. We define an $(l+l')$-system P contained in $Q \cap Q'$ as follows. Let $V = U \cap U'$. Suppose we have defined $V_{v_1,\dots,v_{j-1}}$ for all $j \leq k$. Let $v_1 \in V, v_2 \in V_{v_1}, \dots, v_{k-1} \in V_{v_1,\dots,v_{k-2}}$. We let

$$V_{v_1\dots,v_{k-1}} = U_{v_1\dots,v_{k-1}} \cap U'_{v_1\dots,v_{k-1}}.$$

This is well-defined and has codimension at most $l+l'$ in $\mathbb{F}_2^{n_k}$. Let P be the corresponding $(l+l')$-system. $\square$

Lemma 2.12. *Let $\mathcal{B}' \subset \mathcal{B}$ be a multiset such that $|\mathcal{B}'| \geq \delta|\mathcal{B}|$. Then there exists an $f_1(d,\delta)$-system with elements chosen from $f_2(d)\mathcal{B}'$.*

Proof. The proof is by induction on d. The case $d=1$ is an easy application of Bogolyubov's lemma. Suppose that the lemma has been proved for all $d' < d$ and let $\mathcal{B}' \subset \mathcal{B}$ be a multiset such that $|\mathcal{B}'| \geq \delta|\mathcal{B}|$. Let $\mathcal{D}$ be the multiset $\{v_2 \otimes \cdots \otimes v_d : v_2 \in \mathbb{F}_2^{n_2}, \dots, v_d \in \mathbb{F}_2^{n_d}\}$. For each $u \in \mathbb{F}_2^{n_1}$, let

$$\mathcal{B}'_u = \{s \in \mathcal{D} : u \otimes s \in \mathcal{B}'\} \quad \text{and let} \quad T = \{u \in \mathbb{F}_2^{n_1} : |\mathcal{B}'_u| \geq (\delta/2)|\mathcal{D}|\}.$$

By averaging, we have that $|T| \geq (\delta/2)2^{n_1}$. Now by the induction hypothesis, for every $t \in T$, there exists an $f_1(d-1,\delta/2)$-system P_t in $\mathbb{F}_2^{n_2} \otimes \cdots \otimes \mathbb{F}_2^{n_d}$ (the definition is analogous to the definition of a system in $\mathbb{F}_2^{n_1} \otimes \dots \mathbb{F}_2^{n_d}$), which is contained in $f_2(d-1)\mathcal{B}'_t$. By Bogolyubov's lemma, $4T = 2T - 2T$ contains a subspace $U \subset \mathbb{F}_2^{n_1}$ of codimension at most $g_1(\delta)$. For each $u \in U$, write $u = t_1+t_2+t_3+t_4$ arbitrarily with $t_i \in T$, and let

$$Q_u = P_{t_1} \cap P_{t_2} \cap P_{t_3} \cap P_{t_4},$$

which is a $4f_1(d-1,\delta/2)$-system, by Lemma 2.11. Now $Q = \bigcup_{u \in U}(u \otimes Q_u)$ is an $f_1(d,\delta)$-system provided that $f_1(d,\delta) \geq \max(4f_1(d-1,\delta/2), g_1(\delta))$. Moreover, for any $u \in U, s \in Q_u$, we have $u \otimes s \in 4f_2(d-1)\mathcal{B}'$, so Q is suitable provided that $f_2(d) \geq 4f_2(d-1)$. $\square$

The next lemma is the last ingredient needed to prove that (H') follows from (H).

Lemma 2.13. *Let Q be a k-system, and for each non-empty $I \subset [d]$ let $L_I \subset \mathbb{F}_2^I$ be a subspace of codimension at most l. Let $T = \bigcap_I (L_I \otimes \mathbb{F}_2^{I^c})$. Then $Q \cap T$ contains an $f(d,k,l)$-system.*

Proof. Let the spaces of Q be $U_{u_1,\dots,u_{j-1}}$. It suffices to prove that for every $1 \leq j \leq d$, and every $u_1 \in U, \dots, u_{j-1} \in U_{u_1,\dots,u_{j-2}}$, the codimension of

$$(u_1 \otimes \cdots \otimes u_{j-1} \otimes U_{u_1,\dots,u_{j-1}}) \cap \bigcap_{I \subset [j], j \in I} (L_I \otimes \mathbb{F}_2^{[j]\setminus I})$$

in $u_1 \otimes \cdots \otimes u_{j-1} \otimes U_{u_1,\dots,u_{j-1}}$ is at most $g_1(d,l)$. Thus, it suffices to prove that for every $I \subset [j]$ with $j \in I$, the codimension of

$$(u_1 \otimes \cdots \otimes u_{j-1} \otimes U_{u_1,\dots,u_{j-1}}) \cap (L_I \otimes \mathbb{F}_2^{[j]\setminus I})$$

in $u_1 \otimes \cdots \otimes u_{j-1} \otimes U_{u_1,\dots,u_{j-1}}$ is at most $g_2(l)$. But this is equivalent to the statement that

$$\left(\Big(\bigotimes_{i \in I\setminus\{j\}} u_i\Big) \otimes U_{u_1,\dots,u_{j-1}}\right) \cap L_I$$

has codimension at most $g_2(l)$ in $(\bigotimes_{i\in I\setminus\{j\}} u_i) \otimes U_{u_1,\dots,u_{j-1}}$, which clearly holds with $g_2(l) = l$. □

Lemma 2.14. *If (H) holds for d, then so does (H').*

Proof. Let $\mathcal{B}'$ and L_I be given as in (H'). By Lemma 2.12, we can choose a $g_1(d,\delta)$-system in $g_2(d)\mathcal{B}'$. Thus, by Lemma 2.13,

$$(g_2(d)\mathcal{B}') \cap \bigcap_I (L_I \otimes \mathbb{F}_2^{I^c})$$

contains a $g_3(d,\delta,l)$-system $\mathcal{B}''$. Note that $\mathcal{B}'' \subset \mathcal{B}$ with $|\mathcal{B}''| \geq g_4(d,\delta,l)|\mathcal{B}|$, where $g_4(d,\delta,l) > 0$. By hypothesis (H) applied to $\mathcal{B}''$ in place of $\mathcal{B}'$, it follows that there is a multiset Q, with elements chosen from $\mathcal{B} \cap g_5(d)\mathcal{B}'' \subset \mathcal{B} \cap g_5(d)g_2(d)\mathcal{B}'$, which is $(g_6(d,\delta,l), 1-g_7(d))$-forcing. Now $Q \subset \bigcap_I (L_I \otimes \mathbb{F}_2^{I^c})$, finishing the proof. □

The next result generalizes Lemma 2.5. To state it, we need to find the equivalent of low-rank matrices in the higher-dimensional case. The definition we use is essentially the same as that of the *partition rank* of a tensor (see for example [8] for a discussion of this notion). Indeed, if a tensor has partition rank at most k, then it is k-degenerate (in the sense of the next definition), and conversely if a tensor is k-degenerate, then it has partition rank is at most $2^{d-1}k$.

The second author has shown that the partition rank is also related to the *analytic rank* of a tensor [4, 5], which we do not define here (but again see [8]), with a polynomial dependence, improving on the previously known Ackermann dependence. In this section we use a very similar argument, but since we do not care about bounds, we present it in qualitative form for ease of reading and for the sake of completeness.

Definition 2.15. Let k be a positive integer. We say that $r \in \mathcal{G}$ is *k-degenerate* if there is a collection of subspaces $H_I \subset \mathbb{F}_2^I$, one for each non-empty proper subset $I \subset [d]$ and each one of dimension at most k, such that

$$r \in \sum_{I \subset [d-1], I \neq \emptyset} H_I \otimes H_{I^c}.$$

If $r \in H_I \otimes \mathbb{F}_2^{I^c}$ with $\dim(H_I) \leq k$, then $r \in H_I \otimes H_{I^c}$ for some $H_{I^c} \subset \mathbb{F}_2^{I^c}$ of dimension at most k. (This follows by writing r as $\sum_{j\leq m} s_j \otimes t_j$ with $\{s_j\}$ a basis for H_I and letting H_{I^c} be the span of all t_j.) Thus, r is k-degenerate if and only if we have the apparently weaker condition that

$$r \in \sum_{I \subset [d-1], I \neq \emptyset} H_I \otimes \mathbb{F}_2^{I^c}$$

for some collection of subspaces $H_I \subset \mathbb{F}_2^I$ of dimension at most k, or equivalently the condition that

$$r \in \sum_{I \subset [d-1], I \neq \emptyset} \mathbb{F}_2^I \otimes H_{I^c}$$

for some collection of subspaces $H_{I^c} \subset \mathbb{F}_2^{I^c}$ of dimension at most k.

Lemma 2.16. *Suppose that (H) holds for $d-1$. Let $\mathcal{D}$ be the multiset*

$$\{u_1 \otimes \cdots \otimes u_{d-1} : u_1 \in \mathbb{F}_2^{n_1}, \ldots, u_{d-1} \in \mathbb{F}_2^{n_{d-1}}\}.$$

(i) Let $\mathcal{D}' \subset \mathcal{D}$, and for each $t \in \mathcal{D}'$, let U_t be a subspace of $\mathbb{F}_2^{n_d}$ of codimension at most k with the codimensions of the U_t all equal. Let Q be the multiset $\bigcup_{t \in \mathcal{D}'}(t \otimes U_t)$. If $m = 2^{k+3}$, and $r_1, \ldots, r_m \in \mathcal{G}$ have the property that for every i, $r_i.q = 0$ holds for at least $(3/4)|Q|$ choices of $q \in Q$, then there exist $i \neq j$ such that $(r_i - r_j)(v_1 \otimes \cdots \otimes v_{d-1}) = 0$ for at least $f_1(k)|\mathcal{D}'|$ choices of $v_1 \otimes \cdots \otimes v_{d-1} \in \mathcal{D}'$, where $f_1(k) > 0$ depends only on k.

(ii) Let $c > 0$ and let $r \in \mathcal{G}$ be such that $r(v_1 \otimes \cdots \otimes v_{d-1}) = 0$ for at least $c|\mathcal{D}|$ choices $v_1 \otimes \cdots \otimes v_{d-1} \in \mathcal{D}$. Then r is $f_2(d,c)$-degenerate.

(iii) Let $\delta > 0$ and let $\mathcal{B}' \subset \mathcal{B}$ be such that $|\mathcal{B}'| \geq \delta|\mathcal{B}|$. Then there exists $Q \subset \mathcal{B} \cap 4\mathcal{B}'$ with the following property. If $m \geq f_3(\delta)$ and $r_1, \ldots, r_m \in \mathcal{G}$ are such that for each i, $r_i.q = 0$ for at least $(3/4)|Q|$ choices $q \in Q$, then there exist $i \neq j$ such that $r_i - r_j$ is $f_4(d,\delta)$-degenerate.

(iv) Let $\delta > 0$ and let $\mathcal{B}' \subset \mathcal{B}$ be such that $|\mathcal{B}'| \geq \delta|\mathcal{B}|$. Then there exist $Q \subset \mathcal{B} \cap 4\mathcal{B}'$ and a subspace $V_{[d]} \subset \mathbb{F}_2^{[d]}$ of dimension at most $f_3(\delta)$ with the following property. Any array r with $r.q = 0$ for at least $(3/4)|Q|$ choices $q \in Q$ can be written as $r = x + y$ where $x \in V_{[d]}$ and y is $f_4(d,\delta)$-degenerate.

Proof. (i) By averaging, for every $i \leq m$ there are at least $|\mathcal{D}'|/2$ choices of $t \in \mathcal{D}'$ such that $r_i.(t \otimes u) = 0$ for more than half the $u \in U_t$. But $r_i.(t \otimes u) = (r_i t).u$, so for these t we have that $r_i t \in U_t^{\perp}$. By further averaging, it follows that for at least $|\mathcal{D}'|/4$ choices of $t \in \mathcal{D}'$ we have that $r_i t \in U_t^{\perp}$ for at least $m/4$ choices of $i \leq m$. Since $m/4 > |U_t^{\perp}|$, for every such t, there exist $i \neq j$ with $r_i t = r_j t$. Thus, for some $i \neq j$, there are at least $|\mathcal{D}'|/(4m^2)$ choices of $t \in \mathcal{D}'$ with $r_i t = r_j t$, which implies the statement we wish to prove.

(ii) Write $r = \sum_i s_i \otimes w_i$ where $s_i \in \mathbb{F}_2^{n_1} \otimes \cdots \otimes \mathbb{F}_2^{n_{d-1}}$ and $\{w_i\}$ is a basis for $\mathbb{F}_2^{n_d}$. Note that $r(v_1 \otimes \cdots \otimes v_{d-1}) = 0$ if and only if $s_i.(v_1 \otimes \cdots \otimes v_{d-1}) = 0$ for every i. Let $\mathcal{D}'$ be the multiset consisting of all $v_1 \otimes \cdots \otimes v_{d-1}$ with $s_i.(v_1 \otimes \cdots \otimes v_{d-1}) = 0$ for every i. By assumption, $|\mathcal{D}'| \geq c|\mathcal{D}|$. Since (H) holds for $d-1$, there exists a multiset Q, with elements chosen from $g_1(d)\mathcal{D}'$, which is $(g_2(d,c), 1 - g_3(d))$-forcing. Since $s_i.q = 0$ for every $q \in Q$, it follows that there exist subspaces $V_I \subset \mathbb{F}_2^I$ for every $I \subset [d-1], I \neq \emptyset$, of dimension at most $g_2(d,c)$ such that

$$s_i \in \sum_I V_I \otimes \mathbb{F}_2^{[d-1] \setminus I}$$

for all i. In particular,

$$r \in \sum_{I \subset [d-1], I \neq \emptyset} V_I \otimes \mathbb{F}_2^{I^c}.$$

Thus, r is $g_2(d,c)$-degenerate.

(iii) Let $\mathcal{D}' = \{t \in \mathcal{D} : t \otimes u \in \mathcal{B}'$ for at least $(\delta/2)2^{n_d}$ choices $u \in \mathbb{F}_2^{n_d}\}$. Clearly, we have $|\mathcal{D}'| \geq (\delta/2)|\mathcal{D}|$. Moreover, by Bogolyubov's lemma, for every $t \in \mathcal{D}'$, there exists a subspace $U_t \subset \mathbb{F}_2^{n_d}$ of codimension at most $g_4(\delta)$ such that $t \otimes U_t \subset 4\mathcal{B}'$. After passing to suitable subspaces, we may assume that all U_t have the same codimension. Now let $Q = \bigcup_{t \in \mathcal{D}'}(t \otimes U_t)$. By (i), if $f_3(\delta) \geq 2^{g_4(\delta)+3}$, then there exist $i \neq j$ such that $(r_i - r_j)t = 0$ for at least $g_5(\delta)|\mathcal{D}'|$ choices $t \in \mathcal{D}'$ (where $g_5(\delta) > 0$) and therefore also for at least $g_6(\delta)|\mathcal{D}|$ choices $t \in \mathcal{D}$ (where $g_6(\delta) > 0$). By (ii), it follows that $r_i - r_j$ is $g_7(d,\delta)$-degenerate.

(iv) Choose Q as in (iii) and let $r_1, \dots, r_m$ be a maximal set such that for all i we have $r_i.q = 0$ for at least $(3/4)|Q|$ choices $q \in Q$, and for all $i \neq j$, $r_i - r_j$ is not $f_4(d,\delta)$-degenerate. Then, by (iii), we have $m < f_3(\delta)$. Let $V_{[d]}$ be the span of all the r_i. The result follows by the maximality of $\{r_1, \dots, r_m\}$. □

The next lemma is the key step to complete the proof of Lemma 2.1. In order to state it, we need to introduce a total ordering $\prec$ of the non-empty subsets of $[d-1]$. It does not matter exactly what the ordering is, but we require it to have the property that if $J \subsetneq I$ then $J \prec I$.

To understand the point of the next lemma, observe that we take an array r that belongs to the sum of a certain set of subspaces, some of which depend on r, and we show, using the hypothesis that $r.q = 0$ for almost all $q \in Q$, that it is contained in a similar sum, but with the subspace corresponding to I^c no longer depending on r. By applying this lemma repeatedly, we shall remove all dependence on r from the right-hand side.

Lemma 2.17. *Suppose that (H') holds for every $d' < d$. Let $\delta > 0$ and let $\mathcal{B}' \subset \mathcal{B}$ be such that $|\mathcal{B}'| \geq \delta|\mathcal{B}|$. Let $I \subset [d-1], I \neq \emptyset$ and for each $J \prec I$ let $W_J \subset \mathbb{F}_2^J, W_{J^c} \subset \mathbb{F}_2^{J^c}$ be subspaces of dimension at most k. In addition, let $W_{[d]} \subset \mathbb{F}_2^{[d]}$ be a subspace of dimension at most k. Then there exists a multiset Q with elements chosen from $\mathcal{B} \cap f_1(d)\mathcal{B}'$ with the following property. Any array*

$$r \in W_{[d]} + \sum_{J \prec I}(W_J \otimes \mathbb{F}_2^{J^c} + \mathbb{F}_2^J \otimes W_{J^c}) + \sum_{J \succeq I} \mathbb{F}_2^J \otimes H_{J^c}(r)$$

with $\dim(H_{J^c}(r)) \leq k$ and the property that $r.q = 0$ for at least $(1 - f_2(d))|Q|$ choices $q \in Q$ is contained in a subspace

$$W_{[d]} + \sum_{J \preceq I}(U_J \otimes \mathbb{F}_2^{J^c} + \mathbb{F}_2^J \otimes U_{J^c}) + \sum_{J \succ I} \mathbb{F}_2^J \otimes K_{J^c}(r)$$

for some $U_J \subset \mathbb{F}_2^J, U_{J^c} \subset \mathbb{F}_2^{J^c}$ not depending on r and some $K_{J^c}(r) \subset \mathbb{F}_2^{J^c}$ possibly depending on r, all of dimension at most $f_3(d,\delta,k)$.

Proof. After reordering if necessary, we may assume that $I = [a]$ for some $1 \leq a \leq d-1$. The next claim gives us a multiset Q with certain properties. Once we have it, we shall use those properties to show that Q satisfies the conclusion of the lemma.

Claim. There exist a multiset Q' with elements chosen from

$$\bigcap_{J \subset I, J \neq I, J \neq \emptyset} (W_J^\perp \otimes \mathbb{F}_2^{I \setminus J})$$

which is $(h_1(d,\delta,k), 1-h_2(d))$-forcing (with $h_2(d)>0$), and for each $s\in Q'$, a multiset Q_s with elements chosen from $\mathbb{F}_2^{I^c}$ which is $(h_3(d,\delta), 1-h_4(d))$-forcing (with $h_4(d)>0$) such that $\max_{s\in Q'}|Q_s| \leq 2\min_{s\in Q'}|Q_s|$ and setting Q to be the multiset

$$\{s\otimes t : s\in Q', t\in Q_s\} = \bigcup_{s\in Q'}(s\otimes Q_s),$$

the elements of Q belong to $\mathcal{B}\cap h_5(d)\mathcal{B}'$.

Proof of Claim. Let $\mathcal{C}$ be the multiset $\{u_1\otimes\cdots\otimes u_a : u_i\in\mathbb{F}_2^{n_i}\}$ and let $\mathcal{D}$ be the multiset $\{u_{a+1}\otimes\cdots\otimes u_d : u_i\in\mathbb{F}_2^{n_i}\}$. For each $s\in\mathcal{C}$, let $\mathcal{D}_s=\{t\in\mathcal{D} : s\otimes t\in\mathcal{B}'\}$. Also, let $\mathcal{C}'=\{s\in\mathcal{C} : |\mathcal{D}_s|\geq(\delta/2)|\mathcal{D}|\}$. Clearly, $|\mathcal{C}'|\geq(\delta/2)|\mathcal{C}|$. By Lemma 2.12, for every $s\in\mathcal{C}'$ there exists a $g_1(d,\delta)$-system R_s in $g_2(d)\mathcal{D}_s$. By (H') applied to dimension a, there exists a multiset Q' with elements chosen from

$$\mathcal{C}\cap(g_3(d)\mathcal{C}')\cap\bigcap_{J\subset I, J\neq I, J\neq\emptyset}(W_J^{\perp}\otimes\mathbb{F}_2^{I\setminus J})$$

which is $(g_4(d,\delta,k), 1-g_5(d))$-forcing for some $g_5(d)>0$. For every $s\in Q'$, choose $s_1,\dots,s_l\in\mathcal{C}'$ with $l\leq g_3(d)$ such that $s=s_1+\cdots+s_l$, and let $P_s=\bigcap_{i\leq l}R_s$. By Lemma 2.11, P_s contains a $g_6(d,\delta)$-system, therefore $|P_s|\geq g_7(d,\delta)|\mathcal{D}|$ for some $g_7(d,\delta)>0$. By (H) for $d-a$, for every $s\in Q'$ there exists a multiset Q_s with elements chosen from $\mathcal{D}\cap g_8(d)P_s$ which is $(g_9(d,\delta), 1-g_{10}(d))$-forcing for some $g_{10}(d)>0$. Notice that if we repeat every element of Q_s the same number of times, then the multiset we obtain is still $(g_9(d,\delta), 1-g_{10}(d))$-forcing, so we may assume that $\max_{s\in Q'}|Q_s|\leq 2\min_{s\in Q'}|Q_s|$. Define

$$Q=\{s\otimes t : s\in Q', t\in Q_s\}=\bigcup_{s\in Q'}(s\otimes Q_s).$$

Note that as $R_s\subset g_2(d)\mathcal{D}_s$ for all $s\in\mathcal{C}'$, we have $s\otimes R_s\subset g_2(d)\mathcal{B}'$ for all $s\in\mathcal{C}'$. But the elements of Q' are chosen from $g_3(d)\mathcal{C}'$, so $s\otimes P_s\subset g_3(d)g_2(d)\mathcal{B}'$ for all $s\in Q'$. Finally, the elements of Q_s are chosen from $g_8(d)P_s$, so the elements of $s\otimes Q_s$ are chosen from $g_8(d)g_3(d)g_2(d)\mathcal{B}'$ for every $s\in Q'$. This completes the proof of the claim. $\square$

Now let us show that Q does indeed satisfy the conclusion of the lemma. Since for every $s\in Q'$, Q_s is $(h_3(d,\delta), 1-h_4(d))$-forcing, there exist subspaces $V_J(s)\subset\mathbb{F}_2^J$ for every $J\subset I^c, J\neq\emptyset$, with dimension at most $h_3(d,\delta)$ such that the set of arrays $t\in\mathbb{F}_2^{I^c}$ with $t.q=0$ for at least $(1-h_4(d))|Q_s|$ choices $q\in Q_s$ is contained in

$$\sum_{J\subset I^c, J\neq\emptyset} V_J(s)\otimes\mathbb{F}_2^{I^c\setminus J}.$$

Let $f_2(d)=(1/4)h_2(d)h_4(d)$. Now if $r\in\mathcal{G}$ has $r.q=0$ for at least $(1-f_2(d))|Q|$ choices $q\in Q$, then by averaging, for at least $(1-(1/2)h_2(d))|Q'|$ choices $s\in Q'$, we have $r.(s\otimes t)=0$ for at least $(1-h_4(d))|Q_s|$ choices $t\in Q_s$. Therefore (noting that $r.(s\otimes t)=(rs).t$),

$$rs\in\sum_{J\subset I^c, J\neq\emptyset} V_J(s)\otimes\mathbb{F}_2^{I^c\setminus J}$$

for at least $(1-(1/2)h_2(d))|Q'|$ choices $s\in Q'$.

Now let

$$g_{11}(d,k) = \frac{h_2(d)}{2\cdot 2^k} \qquad \text{and} \qquad g_{12}(d,\delta,k) = h_3(d,\delta) + 2^{d+1}k.$$

Let X be the subset of $\mathbb{F}_2^{I^c}$ consisting of those arrays x such that for at least $g_{11}(d,k)|Q'|$ choices $s \in Q'$, there exists some

$$t(s) \in V_{I^c}(s) + \sum_{J\subset I, J\neq I} ((\mathbb{F}_2^J \otimes W_{J^c})s)$$

for which $x - t(s)$ is $g_{12}(d,\delta,k)$-degenerate. (Here and below, for a subspace $L \subset \mathcal{G}$ and an array $s \in \mathbb{F}_2^I$, we write Ls for the subspace $\{rs : r \in L\} \subset \mathbb{F}_2^{I^c}$.) Choose a maximal subset $\{x_1,\dots,x_m\} \subset X$ such that no $x_i - x_j$ with $i \neq j$ is $2g_{12}(d,\delta,k)$-degenerate. Then there do not exist $i \neq j$, $s \in Q'$ and

$$t \in V_{I^c}(s) + \sum_{J\subset I, J\neq I} ((\mathbb{F}_2^J \otimes W_{J^c})s)$$

with $x_i - t$ and $x_j - t$ both $g_{12}(d,\delta,k)$-degenerate. It follows, by the definition of X and the fact that the dimension of

$$V_{I^c}(s) + \sum_{J\subset I, J\neq I} ((\mathbb{F}_2^J \otimes W_{J^c})s)$$

is at most $h_3(d,\delta) + 2^d k$, that $mg_{11}(d,k)|Q'| \leq |Q'| \cdot 2^{h_3(d,\delta)+2^d k}$, and therefore that $m \leq g_{13}(d,\delta,k)$. Thus, there exists a set $Y \subset X$ of size at most $g_{13}(d,\delta,k)$ such that for any $x \in X$, there exists some $y \in Y$ such that $x - y$ is $2g_{12}(d,\delta,k)$-degenerate. Let $Z = \mathrm{span}(Y)$. Then $\dim(Z) \leq g_{13}(d,\delta,k)$, and for every $x \in X$ there is some $z \in Z$ such that $x - z$ is $2g_{12}(d,\delta,k)$-degenerate.

Let

$$r \in W_{[d]} + \sum_{J \prec I} (W_J \otimes \mathbb{F}_2^{J^c} + \mathbb{F}_2^J \otimes W_{J^c}) + \sum_{J \succeq I} \mathbb{F}_2^J \otimes H_{J^c}(r)$$

with $\dim(H_{J^c}(r)) \leq k$ and the property that $r.q = 0$ for at least $(1 - f_2(d))|Q|$ choices $q \in Q$. Let $Q'(r)$ be the submultiset of Q' consisting of those $s \in Q'$ for which

$$rs \in \sum_{J\subset I^c, J\neq\emptyset} V_J(s) \otimes \mathbb{F}_2^{I^c \setminus J}.$$

As we have seen two paragraphs above,

$$|Q'(r)| \geq \left(1 - \frac{1}{2}h_2(d)\right)|Q'|.$$

Note that we can write $r = r_1 + r_2 + r_3 + r_4$ where

$$r_1 \in \sum_{J\subset I, J\neq I, J\neq\emptyset} W_J \otimes \mathbb{F}_2^{J^c}, \qquad r_2 \in \sum_{J \prec I, J\not\subset I} (W_J \otimes \mathbb{F}_2^{J^c} + \mathbb{F}_2^J \otimes W_{J^c}) + \sum_{J \succ I} \mathbb{F}_2^J \otimes H_{J^c}(r),$$

$$r_3 \in W_{[d]} + \sum_{J\subset I, J\neq I, J\neq\emptyset} \mathbb{F}_2^J \otimes W_{J^c} \quad \text{and} \quad r_4 \in \mathbb{F}_2^I \otimes H_{I^c}(r).$$

Since the elements of Q' belong to

$$\bigcap_{J\subset I, J\neq I, J\neq\emptyset} (W_J^\perp \otimes \mathbb{F}_2^{I\setminus J}),$$

we have $r_1 s = 0$ for every $s \in Q'$.

Since $\dim(W_J), \dim(W_{J^c}), \dim(H_{J^c}(r)) \leq k$, $r_2 s$ is $2^{d+1}k$-degenerate. Indeed, we have $s \in Q'$, so also $s \in \mathcal{C}$, therefore for any $J \subset [d-1]$ we may write $s = s_1 \otimes s_2$ where $s_1 \in \mathbb{F}_2^{I \cap J}$ and $s_2 \in \mathbb{F}_2^{I \cap J^c}$. Then

$$(W_J \otimes \mathbb{F}_2^{J^c})s \subset (W_J s_1) \otimes \mathbb{F}_2^{I^c \cap J^c}.$$

Hence, if $J \not\subset I$, then any tensor in $(W_J \otimes \mathbb{F}_2^{J^c})s$ is k-degenerate. Similarly, any tensor in $(\mathbb{F}_2^J \otimes W_{J^c})s$ or in $(\mathbb{F}_2^J \otimes H_{J^c}(r))s$ is k-degenerate, so $r_2 s$ is indeed $2^{d+1}k$-degenerate.

Also,

$$r_3 s \in \sum_{J \subset I, J \neq I} ((\mathbb{F}_2^J \otimes W_{J^c})s).$$

It follows that for every $s \in Q'(r)$, there exists some

$$t(s) \in V_{I^c}(s) + \sum_{J \subset I, J \neq I} ((\mathbb{F}_2^J \otimes W_{J^c})s)$$

such that $r_4 s - t(s)$ is $g_{12}(d, \delta, k) = (h_3(d, \delta) + 2^{d+1}k)$-degenerate (we have used that $\dim(V_J(s)) \leq h_3(d, \delta)$). In particular, if $t \notin X$, then the number of choices $s \in Q'(r)$ for which $r_4 s = t$ is at most $g_{11}(d, \delta, k)|Q'|$. On the other hand, notice that $r_4 s \in H_{I^c}(r)$ for every $s \in Q'$. Since $|H_{I^c}(r)| \leq 2^k$, it follows that $r_4 s \in X$ for at least

$$|Q'(r)| - 2^k g_{11}(d, \delta, k)|Q'| = |Q'(r)| - \frac{1}{2}h_2(d)|Q'| \geq (1 - h_2(d))|Q'|$$

choices $s \in Q'$.

Let $X(r) = X \cap H_{I^c}(r)$. Let $t_1, \dots, t_\alpha$ be a maximal linearly independent subset of $X(r)$ and extend it to a basis $t_1, \dots, t_\alpha, t'_1, \dots, t'_\beta$ for $H_{I^c}(r)$. Now if a linear combination of $t_1, \dots, t_\alpha, t'_1, \dots, t'_\beta$ is in X, then the coefficients of $t'_1, \dots, t'_\beta$ are all zero. Write $r_4 = \sum_{i \leq \alpha} s_i \otimes t_i + \sum_{j \leq \beta} s'_j \otimes t'_j$ for some $s_i, s'_j \in \mathbb{F}_2^I$. Since $r_4 q \in X$ for at least $(1 - h_2(d))|Q'|$ choices $q \in Q'$, we have, for all j, that $s'_j.q = 0$ for at least $(1 - h_2(d))|Q'|$ choices $q \in Q'$. Thus, as Q' is $(h_1(d, \delta, k), 1 - h_2(d))$-forcing, there exist subspaces $L_J \subset \mathbb{F}_2^J$ ($J \subset I, J \neq \emptyset$), not depending on r and of dimension at most $h_1(d, \delta, k)$, such that

$$s'_j \in \sum_{J \subset I, J \neq \emptyset} L_J \otimes \mathbb{F}_2^{I \setminus J}$$

for all j. Thus,

$$r_4 \in \sum_{i \leq \alpha} s_i \otimes t_i + \sum_{J \subset I, J \neq \emptyset} L_J \otimes \mathbb{F}_2^{J^c}.$$

Moreover, for every $i \leq \alpha$, we have $t_i \in X$, so there exist $z_i \in Z$ such that $t_i - z_i$ is $2g_{12}(d, \delta, k)$-degenerate. It follows that

$$r_4 \in \mathbb{F}_2^I \otimes Z + \sum_{J \supset I, J \neq I, J \subset [d-1]} \mathbb{F}_2^J \otimes K'_{J^c}(r) + \sum_{J \subset I, J \neq \emptyset} L_J \otimes \mathbb{F}_2^{J^c}$$

for some $K'_{J^c}(r) \subset \mathbb{F}_2^{J^c}$ of dimension at most $\alpha \cdot 2g_{12}(d, \delta, k) \leq 2^k \cdot 2g_{12}(d, \delta, k)$. This finishes the proof of the lemma. □

We are now in a position to complete the proof of Lemma 2.1.

Proof of Lemma 2.1. As remarked earlier, it suffices to prove that (H) holds for all d. But (H) implies (H'), and (H) holds for $d=1$, therefore it suffices to prove, assuming that (H') holds for all $d'<d$, that (H) holds for d.

Let $\mathcal{B}'$ given as in the definition of (H). By Lemma 2.16 (iv), there exist $Q_\emptyset \subset \mathcal{B} \cap 4\mathcal{B}'$ and $V_{[d]} \subset \mathbb{F}_2^{[d]}$ of dimension at most $g_1(\delta)$ such that if $r.q=0$ for at least $(3/4)|Q_\emptyset|$ choices $q \in Q_\emptyset$, then r can be written as $r=x+y$, where $x \in V_{[d]}$ and y is $g_2(d,\delta)$-degenerate. By repeated application of Lemma 2.17, for all $I \subset [d-1]$ with $I \neq \emptyset$, in the order given by $\prec$, we obtain for each such I a multiset Q_I with elements chosen from $\mathcal{B} \cap g_3(d)\mathcal{B}'$, subspaces $V_I \subset \mathbb{F}_2^I$, $V_{I^c} \subset \mathbb{F}_2^{I^c}$ of dimension at most $g_4(d,\delta)$, and we also obtain a constant $g_5(d)>0$ such that the following statement holds. If $r \in \mathcal{G}$ is such that for each $I \subset [d-1]$ we have that $r.q=0$ for at least $(1-g_5(d))|Q_I|$ choices of $q \in Q_I$, then

$$r \in V_{[d]} + \sum_{I \subset [d-1], I \neq \emptyset} (V_I \otimes \mathbb{F}_2^{I^c} + \mathbb{F}_2^I \otimes V_{I^c}).$$

Moreover, after taking several copies of each Q_I, we may assume that $\max_I |Q_I| \leq 2\min_I |Q_I|$. Now let

$$g_6(d) = \frac{g_5(d)}{2 \cdot 2^{d-1}},$$

let $Q = \bigcup_I Q_I$, and suppose that $r.q=0$ for at least $(1-g_6(d))|Q|$ choices $q \in Q$. Then, by averaging, for every $I \subset [d-1]$ we have $r.q=0$ for at least $(1-g_5(d))|Q_I|$ choices of $q \in Q_I$. Thus, Q is $(g_7(d,\delta), 1-g_6(d))$-forcing, where $g_7(d,\delta) = \max(g_1(\delta), g_4(d,\delta))$. □

3 The counterexample to Question 1.9

We shall now present an example that gives a negative answer to Question 1.9. The example is easy to define, but it takes a little work to prove that it has the properties we require. In what follows, let $G = \mathbb{F}_2^n$. For a vector $v \in G$ write $|v|$ for the number of entries equal to 1 in v. Then our set A will be $\{v \in \mathbb{F}_2^n : |v| \leq n/2 - 10^{20}n^{3/4}\}$, and our set B will be $\{v \in \mathbb{F}_2^n : |v| = n^{1/2}\}$.

We prove that A is η-closed with respect to B where $\eta > 0$ is some absolute constant.

First we show that when n is sufficiently large, the probability that a uniformly random element $u \in A$ has $|u| \leq n/2 - 10^{20}n^{3/4} - 10^{50}n^{1/4}$ is at least some absolute constant $\eta_1 > 0$. Note that

$$\frac{\binom{n}{k}}{\binom{n}{k+l}} = \frac{(k+1)(k+2)\cdots(k+l)}{(n-k-l+1)(n-k-l+2)\cdots(n-k)} \geq \left(\frac{k}{n-k}\right)^l$$

When $k \geq n/2 - 10^{21}n^{3/4}$, then $(\frac{k}{n-k})^l \geq (\frac{n/2-10^{21}n^{3/4}}{n/2+10^{21}n^{3/4}})^l = (\frac{n^{1/4}/2-10^{21}}{n^{1/4}/2+10^{21}})^l = (1-\frac{2\cdot 10^{21}}{n^{1/4}/2+10^{21}})^l$. It is not hard to see that when $l = 10^{50}n^{1/4}$, then this is at least some absolute constant $c>0$. This means that

$$\sum_{i=0}^{10^{50}n^{1/4}} \binom{n}{n/2 - 10^{20}n^{3/4} - 10^{50}n^{1/4} - i} \geq c \sum_{i=0}^{10^{50}n^{1/4}} \binom{n}{n/2 - 10^{20}n^{3/4} - i},$$

which implies that the probability that a uniformly random element $u \in A$ has $|u| \leq n/2 - 10^{20}n^{3/4} - 10^{50}n^{1/4}$ is at least some absolute constant $\eta_1 > 0$.

We now show that when n is sufficiently large, $u \in \mathbb{F}_2^n$ has $|u| \leq n/2 - 10^{20}n^{3/4} - 10^{50}n^{1/4}$ and $v \in B$ is uniformly randomly chosen, then with probability at least $1/2$, we have $u + v \in A$. For simplicity we assume that $|u| = n/2 - 10^{20}n^{3/4} - 10^{50}n^{1/4}$. Then it suffices to prove that with probability at least $1/2$, we have

$$u \cdot v \geq \frac{n^{1/2}}{2} - 10^{40}n^{1/4}, \tag{3.1}$$

where to define the dot product we view u and w as elements of $\mathbb{R}^n$.

Let $m = n^{1/2}$ and let $w_1, \ldots, w_m$ be standard basis vectors of $\mathbb{F}_2^n$, chosen independently and uniformly at random. Note that the expected number of $i \neq j$ such that $w_i = w_j$ is at most 1, so almost surely this number is at most $\log n$. In particular, almost surely we have $n^{1/2} - 2\log n \leq |w_1 + \cdots + w_m| \leq n^{1/2}$. Choose uniformly randomly an element $v \in B$ with minimal Hamming distance from $w_1 + \cdots + w_m \in \mathbb{F}_2^n$. This algorithm defines a uniformly random element of $v \in B$, and almost surely $u \cdot v \leq u \cdot w_1 + \cdots + u \cdot w_m + 4\log n$. However, $u \cdot w_1 + \cdots + u \cdot w_m$ is distributed as $\mathrm{Bin}(n^{1/2}, 1/2 - 10^{20}n^{-1/4} - 10^{50}n^{-1/2})$. By Chernoff's inequality, this is at least $\frac{n^{1/2}}{2} - 10^{30}n^{1/4}$ with probability at least $9/10$, say, so equation (3.1) holds with probability more than $1/2$. Hence, A is indeed (B, η)-closed for some positive absolute constant η.

What we shall prove next is that for this η, with $\varepsilon = 0.99$, say, there do not exist c, δ and l with the properties described in Question 1.9. In fact, we shall prove the slightly stronger statement that for any $\delta > 0$ and positive integer l, if n is sufficiently large then there do not exist $C \subset A + lB$ and $B' \subset B$ with $|B'| \geq \delta|B|$ such that C is $(B', 0.99)$-closed. Since for sufficiently large n, we have $A + lB \subset A' = \{v \in \mathbb{F}_2^n : |v| \leq n/2 - 10^{15}n^{3/4}\}$, it suffices to prove the same statement but with $A + lB$ replaced by A'. From now on, we always assume that n is sufficiently large.

The proof relies on two lemmas and a definition.

Lemma 3.1. *If $B' \subset B$ has $|B'| \geq \delta|B|$, then $\widehat{\mu_{B'}}(u) \geq 0.98$ for at most $\exp(n^{2/3})$ vectors $u \in \mathbb{F}_2^n$.*

Definition 3.2. Given $B' \subset B$, we say $u \in A'$ is *B'-compatible* if the number of $w \in B'$ with $|u + w| \leq |u|$ is at least $|B'|/3$.

Note that if we fix some $u \in A'$ and take a random $w \in B$, then the probability that $|u + w| \leq |u|$ is much less than $1/3$. Indeed, writing X for the expected number of indices i for which $w_i = 1$ and $u_i = 0$, and Y for the expected number of indices i for which $w_i = 1$ and $u_i = 1$, we have $\mathbb{E}[X - Y] \geq 2 \cdot 10^{15}n^{1/4}$, while the standard deviation of $X - Y$ is around $n^{1/4}$. So $X \leq Y$ holds with quite small probability.

Thus, for any large $B' \subset B$, intuitively we expect only a small proportion of elements of A' to be B'-compatible. The next lemma makes this precise.

Lemma 3.3. *Let $B' \subset B$ have $|B'| \geq \delta|B|$. Then the number of those $u \in A'$ which are B'-compatible is at most $\exp(-n^{3/4})|A'|$.*

Let us see why these two lemmas are sufficient. Suppose that $C \subset A'$ is $(B', 0.99)$-closed for some $B' \subset B$ with $|B'| \geq \delta|B|$. Let $w \in B'$ be chosen at random. Then the expected number of $u \in C$ such that $u + w \in C$ is at least $0.99|C|$, so by considering all such pairs $\{u, u + w\}$ and noting that $(u + w) + w = u$, we see that there are on average at least $(0.99/2)|C|$ choices of $u \in C$ such that $|u+w| \leq |u|$. Therefore, if $u \in C$ is chosen at random, the average number of $w \in B'$ such that $|u+w| \leq |u|$ is at least $(0.99/2)|B'|$. It follows that for at least $|C|/10$ elements of C the number of such w is at least $|B'|/3$, so at least $|C|/10$ elements of A' are B'-compatible. Lemma 3.3 then implies that C has density at most $10\exp(-n^{3/4})$ in G. Let us write γ for this density.

On the other hand, since C is $(B', 0.99)$-closed, we have the inequality

$$\sum_{u \in G} \widehat{\mu_{B'}}(u)|\hat{C}(u)|^2 \geq 0.99 \sum_{u \in G} |\hat{C}(u)|^2,$$

which implies that

$$\sum_{u \in G : \widehat{\mu_{B'}}(u) \geq 0.98} \widehat{\mu_{B'}}(u)|\hat{C}(u)|^2 \geq 0.01 \sum_{u \in G} |\hat{C}(u)|^2.$$

Using Lemma 3.1, together with the observations that $\widehat{\mu_{B'}}(u) \leq 1$ and $|\hat{C}(u)| \leq \gamma$ for every $u \in G$ and that $\sum_{u \in G} |\hat{C}(u)|^2 = \gamma$, we deduce that $\exp(n^{2/3})\gamma^2 \geq 0.01\gamma$, so $\gamma \geq 0.01\exp(-n^{2/3})$. For sufficiently large n, this contradicts the upper bound for γ that we obtained a few lines above.

It remains to prove the two lemmas. The next two results are preparation for the proof of Lemma 3.1.

Lemma 3.4. *Let V be a subspace of $\mathbb{F}_2^n$ of dimension d such that every $v \in V$ has $|v| \geq n^{8/15}$. Then V has a basis $\{v_1, \dots, v_d\}$ such that for every i, the set $I_i = \{k \leq n : v_i(k) = 1, v_j(k) = 0 \text{ for all } j \neq i\}$ has size at least $n^{8/15}/2^{d-1}$. Here and below, the kth entry of a vector v is denoted by $v(k)$.*

Proof. We use induction on d. The case $d = 1$ easily follows from the assumption on V. Let V' have dimension $d+1$ and suppose that for a d-dimensional subspace $V \subset V'$, $v_1, \dots, v_d$ and $I_1, \dots, I_d$ have been chosen satisfying the requirements. Choose some $v \in V' \setminus V$. Replacing v by $v - v_1$ if necessary, we may assume that $v(k) = 0$ for at least $|I_1|/2$ choices $k \in I_1$. Similarly, we may assume that $v(k) = 0$ for at least $|I_i|/2$ choices $k \in I_i$ for every $i \leq d$. Thus, there exist subsets $J_1, \dots, J_d$ of $\{1, \dots, n\}$ of size at least $n^{8/15}/2^d$ each such that for every $i \leq d$ and every $k \in J_i$ we have $v_i(k) = 1$ but $v_j(k) = 0$ for all j with $j \neq i, j \leq d$, and $v(k) = 0$. Let $J = \{k \leq n : v(k) = 1\}$. By the assumption on V', we have $|J| \geq n^{8/15}$. Now it is easy to see that we can define v_1' to be v_1 or $v_1 - v$ and achieve that $v_1'(k) = 0$ for at least $|J|/2$ choices of $k \in J$. Similarly, we can define $v_2', \dots, v_d'$ such that each v_i' is v_i or $v_i - v$ and $v_1'(k) = \cdots = v_d'(k) = 0$ for at least $|J|/2^d$ choices $k \in J$. Then for any $i, j \leq d$, we have $v_i'(k) = v_i(k)$ for every $k \in J_j$, and it follows that for any $i \leq d$ and $k \in J_i$, we have $v_i'(k) = 1$ but $v_j'(k) = 0$ for all $j \neq i$, and $v(k) = 0$. Thus, the set $\{v_1', \dots, v_d', v\}$ is suitable so the lemma is proved. □

Corollary 3.5. *Let t be a positive integer not depending on n and let V be a subspace of $\mathbb{F}_2^n$ of dimension t such that every $v \in V$ has $|v| \geq n^{8/15}$. Then the density of those $w \in B$ with $w \cdot v = 0$ for all $v \in V$ is less than $(1.9)^{-(t-1)}$.*

Proof. We shall be slightly sketchy about the some of the details when they are very standard. As always, we assume that n is sufficiently large. Let $v_1, \dots, v_t$ be a basis given by Lemma 3.4 with $d = t$. Let w be a random vector in B, let $i < t$, and let us consider the probability that $w.v_i = 0$ given that $w.v_j = 0$ for every $j < i$.

The expected number of non-zero coordinates of w in the union of the two intervals I_i and I_{i+1} is at least $n^{1/30}/2^{t-1}$, which tends to infinity, and the probability that it is at least half this number tends to 1 (very rapidly). If we condition further on this number, and if it is indeed at least $n^{1/30}/2^t$, then the probability that the number of non-zero coordinates of w in I_i is even is almost exactly 1/2. Therefore, the probability that $w.v_i = 0$ given that $w.v_j = 0$ for every $j < i$ is less than $1/(1.9)$.

Since this is true for every $i \le t-1$, we obtain the result. $\square$

Proof of Lemma 3.1. Suppose that the result is not true. Let r be a positive integer to be specified later and pick $R = \{u_1, \ldots, u_r\}$ such that $\widehat{\mu_{B'}}(u_i) \ge 0.98$ for $i = 1, 2, \ldots, r$. Then for each i, we have $u_i \cdot w = 0$ for at least 99% of all $w \in B'$. Therefore there is a subset $B'' \subset B'$ with $|B''| \ge |B'|/2$ such that each $w \in B''$ has $u_i \cdot w = 0$ for at least 98% of the u_i. The number of subsets of R of size $(49/50)r$ is at most

$$\binom{r}{49r/50} = \binom{r}{r/50} \le (50\mathrm{e})^{r/50} \le (1.8)^{49r/50}.$$

Let $t = 49r/50$. Then there exists a subset T of R of size t such that the number of $w \in B$ with $w \cdot u = 0$ for all $u \in T$ is at least

$$\frac{|B''|}{(1.8)^t} \ge \frac{\delta}{2 \cdot (1.8)^t}|B|.$$

Choose the smallest positive integer t with

$$\frac{\delta}{2 \cdot (1.8)^t} \ge (1.9)^{-(t-1)}$$

(and with $r = 50t/49$ an integer). Then the density of those $w \in B$ with $w \cdot u = 0$ for all $u \in T$ is at least $(1.9)^{-(t-1)}$.

Now let Q be the set of all $u \in \mathbb{F}_2^n$ with $\widehat{\mu_{B'}}(u) \ge 0.98$ and assume that $|Q| \ge \exp(n^{2/3})$. Let t and r be as above and choose $u_1, \ldots, u_r \in Q$ such that for every j, the (Hamming) distance of u_j from $\mathrm{span}(u_1, \ldots, u_{j-1})$ is at least $n^{8/15}$. (This is possible because the number of $u \in \mathbb{F}_2^n$ with Hamming distance at most $n^{8/15}$ from an r-dimensional vector space is at most $2^r \exp(O(n^{8/15} \log n)) < \exp(n^{2/3})$.) Applying Corollary 3.5 to $V = \mathrm{span}(T)$, where T is a subset of $\{u_1, \ldots, u_r\}$ of size t, we find that the density of those $w \in B$ with $w \cdot u = 0$ for all $u \in T$ is less than $(1.9)^{-(t-1)}$, which is a contradiction. $\square$

Proof of Lemma 3.3. In this proof, unless specified otherwise, we will view $\mathbb{F}_2^n$ as a subset of $\mathbb{R}^n$ and accordingly, the dot product is defined as $u \cdot w = \sum_i u(i)w(i)$ where the summation is in $\mathbb{R}$. Then $|u + w| \le |u|$ is equivalent to $u \cdot w \ge |w|/2$. Hence u is B'-compatible if $u \cdot w \ge |w|/2$ for at least $|B'|/3$ vectors $w \in B'$.

Let t be a fixed positive integer, not depending on n, to be specified later. For a multiset $T = \{u_1, \ldots, u_t\} \subset A'$ write $s_T = \sum_{i=1}^t u_i - (t/2)q$ where q is the vector in $\mathbb{F}_2^n$ consisting of ones. Let $a_k = s_T(k)$ and $\sigma_T^2 = \sum_{k=1}^n a_k^2$. We say that T is *bad* if $\sigma_T^2 \ge 1000tn$.

Claim 1. If T is not bad, then the number of $w \in B$ with $u_i \cdot w \ge |w|/2$ for all i is at most $|B|/100^t$.

Proof of Claim 1. If $u_i \cdot w \ge |w|/2$ for all i, then $s_T \cdot w \ge 0$. Note that $s_T \cdot w = \sum_{k \le n} a_k w(k)$. We shall view w as a random variable, chosen uniformly of all elements of B. What we need to prove is that

$$\mathbb{P}\left[\sum_{k \le n} a_k w(k) \ge 0\right] \le \frac{1}{100^t}.$$

Let $m = n^{1/2}$ and let $w_1, \dots, w_m$ be standard basis vectors of $\mathbb{F}_2^n$, chosen independently and uniformly at random. Note that the expected number of $i \neq j$ such that $w_i = w_j$ is at most 1, so almost surely this number is at most $\log n$. In particular, almost surely we have $n^{1/2} - 2\log n \leq |w_1 + \cdots + w_m| \leq n^{1/2}$. Choose uniformly randomly an element $w \in B$ with minimal Hamming distance from $w_1 + \cdots + w_m \in \mathbb{F}_2^n$. This algorithm defines a uniformly random element of $w \in B$ such that almost surely we have

$$\begin{aligned}\sum_{k \leq n} \left| \sum_{i \leq m} w_i(k) - w(k) \right| &\leq \sum_{k \leq n} \left| \sum_{i \leq m} w_i(k) - \left(\sum_{i \leq m} w_i \right)(k) \right| + \sum_{k \leq n} \left| \left(\sum_{i \leq m} w_i \right)(k) - w(k) \right| \\ &\leq 2\log n + 2\log n = 4\log n,\end{aligned}$$

where all the summations are taken in $\mathbb{R}$, except $\sum_{i \leq m} w_i$, which is taken in $\mathbb{F}_2^n$.

At this point, we apply the following version of Chernoff's inequality, which appears as Theorem 3.4 in [2].

Let X_i ($1 \leq i \leq m$) be independent random variables satisfying $X_i \leq \mathbb{E}[X_i] + M$, for $1 \leq i \leq m$. We consider the sum $X = \sum_i X_i$ with expectation $\mathbb{E}[X] = \sum_i \mathbb{E}[X_i]$ and variance $\operatorname{Var}(X) = \sum_i \operatorname{Var}(X_i)$. Then, we have

$$\mathbb{P}(X \geq \mathbb{E}[X] + \lambda) \leq \exp\left(-\frac{\lambda^2}{2(\operatorname{Var}(X) + M\lambda/3)} \right).$$

We now take $X_i = \sum_{k \leq n} a_k w_i(k)$ for $1 \leq i \leq m$. Since $|a_k| \leq t$, the conditions of the theorem hold with $M = 2t$. As $u_i \in A'$ for all i, we have $\sum_{k \leq n} a_k \leq t(n/2 - 10^{15} n^{3/4}) - tn/2 = -10^{15} t n^{3/4}$. Then

$$\mathbb{E}[X] = m \frac{\sum_{k \leq n} a_k}{n} \leq -\frac{1}{2} 10^{15} t n^{1/4},$$

and by the assumption that T is not bad,

$$\operatorname{Var}(X) \leq m \frac{\sum_{k \leq n} a_k^2}{n} \leq 1000 t n^{1/2}.$$

Thus, taking $\lambda = 10^{14} t n^{1/4}$ in the above theorem it follows that

$$\mathbb{P}\left[\sum_{i \leq m} \sum_{k \leq n} a_k w_i(k) \geq -10^{14} t n^{1/4} \right] \leq \exp\left(-\frac{10^{28} t^2 n^{1/2}}{2(1000 t n^{1/2} + 2t \cdot 10^{14} t n^{1/4}/3)} \right) \leq \frac{1}{2 \cdot 100^t}.$$

But

$$\begin{aligned}\sum_{k \leq n} a_k w(k) &= \sum_{i \leq m, k \leq n} a_k w_i(k) + \sum_{k \leq n} a_k (w(k) - \sum_{i \leq m} w_i(k)) \\ &\leq \sum_{i \leq m, k \leq n} a_k w_i(k) + t \sum_{k \leq n} \left| (w(k) - \sum_{i \leq m} w_i(k)) \right|,\end{aligned}$$

and $\sum_{k \leq n} |(w(k) - \sum_{i \leq m} w_i(k))| \leq 4\log n$ almost surely, it follows that

$$\mathbb{P}\left[\sum_{k \leq n} a_k w(k) \geq 0 \right] \leq \frac{1}{100^t}$$

and Claim 1 is proved.

Claim 2. If $u_1,u_2,\dots,u_t$ are independently and uniformly randomly chosen elements of A' then the probability that $T=\{u_1,\dots,u_t\}$ is bad is $o(\exp(-n^{7/8}))$.

Proof of Claim 2. Recall that T is bad if and only if

$$\sum_{k\le n}\left(\sum_{i\le t}u_i(k)-t/2\right)^2\ge 1000tn.$$

$u_1,\dots,u_t$ are randomly chosen from A' but with probability $1-o(\exp(n^{-7/8}))$ all of them have $|u_i|\ge n/2-n^{99/100}$ so we may assume that $u_1,\dots,u_t$ are randomly chosen from the set

$$A''=\{v\in\mathbb{F}_2^n : n/2-n^{99/100}\le|v|\le n/2-10^{15}n^{3/4}\}.$$

It is not hard to see that we can write $u_i=x_i+y_i$ where x_i and y_i are random variables taking values in $\mathbb{F}_2^n$ and having the property that $x_i(k)$ are independent Bernoulli with parameter $1/2$ and $|y_i|\le 2n^{99/100}$ with probability $1-o(\exp(-n^{7/8}))$. Then it suffices to prove that

$$\mathbb{P}\left[\sum_{k\le n}\left(\sum_{i\le t}x_i(k)-t/2\right)^2\ge 500tn\right]=o(\exp(-n^{7/8})).$$

Let $X_i=(\sum_{i\le t}x_i(k)-t/2)^2$ for $1\le k\le n$. Then the X_i are i.i.d. random variables with $\mathbb{E}[X_i]=t/4$ and $\mathrm{Var}(X_i)=O(1)$. Thus, by Theorem 3.4 from [2] (which is the theorem stated above), taking $\lambda=100tn$ and $M=t^2$, it follows that

$$\mathbb{P}\left[\sum_{k\le n}\left(\sum_{i\le t}x_i(k)-t/2\right)^2\ge 500tn\right]\le\exp\left(-\frac{(100tn)^2}{2(nO(1)+t^2\cdot 100tn/3)}\right)=o(\exp(-n^{7/8})),$$

finishing the proof of Claim 2.

We are now in a position to complete the proof of the lemma. Let t be the smallest positive integer with

$$\frac{1}{100^t}<\frac{\delta}{100(6\mathrm{e})^t}.$$

Let the density of B'-compatible elements in A' be α. Pick $v_1,\dots,v_{6t}$ independently and uniformly randomly from A'. Then with probability α^{6t}, every v_i is B'-compatible. If that is the case, then for every i, there are at least $|B'|/3$ vectors $w\in B'$ with $v_i\cdot w\ge|w|/2$. It follows that there is some $B''\subset B'$ with $|B''|\ge|B'|/100$ such that for every $w\in B''$ we have $v_i\cdot w\ge|w|/2$ for at least t choices of i. The number of t-sets in $\{v_1,\dots,v_{6t}\}$ is at most $(6\mathrm{e})^t$ so there must exist a t-set $T=\{u_1,\dots,u_t\}\subset\{v_1,\dots,v_{6t}\}$ (multisets are allowed) such that the number of $w\in B$ with $u_i\cdot w\ge|w|/2$ for each i is at least

$$\frac{|B''|}{(6\mathrm{e})^t}\ge\frac{\delta|B|}{100(6\mathrm{e})^t}>\frac{|B|}{100^t}.$$

By Claim 1, it follows that T is bad. Thus, the probability that $T=\{u_1,\dots,u_t\}$ is bad when $u_1,\dots,u_t$ are independently and uniformly randomly chosen from A', is at least $\alpha^{6t}/\binom{6t}{t}$. Hence, by Claim 2, we have $\alpha^{6t}/\binom{6t}{t}=o(\exp(-n^{7/8}))$, and we get $\alpha=o(\exp(-n^{3/4}))$. □

Acknowledgement

We are grateful to both referees for their valuable suggestions.

References

[1] BOAZ BARAK, PRAVESH K. KOTHARI, AND DAVID STEURER: Small-set expansion in Shortcode Graph and the 2-to-2 Conjecture, 2019. [doi:10.4230/LIPIcs.ITCS.2019.9, arXiv:1804.08662] 3

[2] FAN CHUNG AND LINYUAN LU: Concentration inequalities and martingale inequalities: A survey. *Internet Mathematics*, 3(1):79–127, 2006. Available at Project Euclid. 26, 27

[3] BEN GREEN: The asymmetric Balog-Szemerédi-Gowers theorem. Lecture notes. 5

[4] OLIVER JANZER: Low analytic rank implies low partition rank for tensors, 2018. [arXiv:1809.10931] 16

[5] OLIVER JANZER: Polynomial bound for the partition rank vs the analytic rank of tensors, 2019. [arXiv:1902.11207] 16

[6] SUBHASH KHOT: On the power of unique 2-prover 1-round games. In *Proc. 34th STOC*, pp. 767–775. ACM Press, 2002. [doi:10.1145/509907.510017] 2

[7] SUBHASH KHOT, DOR MINZER, AND MULI SAFRA: Pseudorandom sets in Grassmann graph have near-perfect expansion. In *Proc. 59th FOCS*, pp. 592–601. IEEE Comp. Soc. Press, 2018. [doi:10.1109/FOCS.2018.00062] 2

[8] SHACHAR LOVETT: The analytic rank of tensors and its applications. *Discrete Analysis*, 2019:7, 10 pp. [doi:10.19086/da.8654, arXiv:1806.09179v5] 16

[9] TERENCE TAO AND VAN H. VU: *Additive Combinatorics*. Cambridge Univ. Press, 2006. [doi:10.1017/CBO9780511755149] 5, 12

AUTHORS

Timothy Gowers
Professor
Department of Pure Mathematics and Mathematical Statistics
University of Cambridge
w.t.gowers@dpmms.cam.ac.uk

Oliver Janzer
Graduate student
Department of Pure Mathematics and Mathematical Statistics
University of Cambridge
oj224@cam.ac.uk
https://sites.google.com/view/oliver-janzer/home

ABOUT THE AUTHORS

TIMOTHY GOWERS was an undergraduate at the University of Cambridge, where he also did his Ph. D. under the supervision of Béla Bollobás. His main research interest is combinatorics, particularly those parts that lie at the interface with other areas of mathematics. He is a Royal Society Research Professor, and holds this position at the University of Cambridge.

OLIVER JANZER grew up in Budapest, Hungary. He obtained his Bachelor and Masters degrees at the University of Cambridge, where he is currently a Ph. D. student of Timothy Gowers. His main research interests are extremal graph theory and additive combinatorics.