Factoring Polynomials over Finite Fields with Linear Galois Groups: An Additive Combinatorics Approach

Zeyu Guo[1]
Department of Computer Science, University of Haifa, Israel
zguotcs@gmail.com

Abstract

Let $\tilde{f}(X) \in \mathbb{Z}[X]$ be a degree-n polynomial such that $f(X) := \tilde{f}(X) \bmod p$ factorizes into n distinct linear factors over $\mathbb{F}_p$. We study the problem of *deterministically* factoring $f(X)$ over $\mathbb{F}_p$ given $\tilde{f}(X)$. Under the generalized Riemann hypothesis (GRH), we give an improved deterministic algorithm that computes the complete factorization of $f(X)$ in the case that the Galois group of $\tilde{f}(X)$ is (permutation isomorphic to) a *linear group* $G \leq \mathrm{GL}(V)$ on the set S of roots of $\tilde{f}(X)$, where V is a finite-dimensional vector space over a finite field $\mathbb{F}$ and S is identified with a subset of V. In particular, when $|S| = |V|^{\Omega(1)}$, the algorithm runs in time polynomial in $n^{\log n/(\log\log\log\log n)^{1/3}}$ and the size of the input, improving Evdokimov's algorithm. Our result also applies to a general Galois group G when combined with a recent algorithm of the author.

To prove our main result, we introduce a family of objects called *linear m-schemes* and reduce the problem of factoring $f(X)$ to a combinatorial problem about these objects. We then apply techniques from additive combinatorics to obtain an improved bound. Our techniques may be of independent interest.

2012 ACM Subject Classification Mathematics of computing → Computations in finite fields; Mathematics of computing → Computations on polynomials; Mathematics of computing → Combinatoric problems; Computing methodologies → Algebraic algorithms

Keywords and phrases polynomial factoring, permutation group, finite field, algebraic combinatorics, additive combinatorics, derandomization

Acknowledgements The author is grateful to Nitin Saxena for helpful discussions.

1 Introduction

Univariate polynomial factoring over finite fields is a fundamental problem in computer algebra, which has been extensively studied over the years. A longstanding open problem in this area is finding a *deterministic* algorithm that factors a degree-n polynomial $f(X)$ over a finite field $\mathbb{F}_q$ in time polynomial in n and $\log q$. There is a long list of work on this problem [1, 5, 6, 34, 38, 29, 30, 28, 35, 36, 20, 21, 9, 31, 10, 8, 13, 23, 15, 22, 2, 3, 7]. In particular, Berlekamp [6] gave a deterministic factoring algorithm that runs in time $\mathrm{poly}(n, \log q, \mathrm{char}(\mathbb{F}_q))$. Building the work of Rónyai [29], Evdokimov [10] gave a deterministic $\mathrm{poly}(n^{\log n}, \log q)$-time algorithm under the generalized Riemann hypothesis (GRH).

Efforts were made to understand the combinatorics behind Evdokimov's algorithm [8, 13], culminating in the work [23] that proposed the notion of *m-schemes* together with an algorithm that subsumes those in [29, 10]. See also the follow-up work [2, 3]. An m-scheme, parameterized by $m \in \mathbb{N}^+$, can be seen as an extension of the notion of *association schemes* in algebraic combinatorics. It was shown in [23] that whenever the algorithm fails to produce a proper factorization of $f(X)$ in time $\mathrm{poly}(n^m, \log q)$, there always exists an m-scheme on

[1] This work was done while the author was at the CSE department, IIT Kanpur.

$[n]$ satisfying strict combinatorial properties. Evdokimov's result can then be interpreted as the fact that such an m-scheme exists only for $m = O(\log n)$. Thus, one natural way of beating Evdokimov's $\mathrm{poly}(n^{\log n}, \log q)$-time algorithm is improving this $O(\log n)$ upper bound for m. However, attempts of establishing an $o(\log n)$ upper bound for m have be unsuccessful so far. Currently, the best known general upper bound is $m \leq c \log n + O(1)$, where $c = 2/\log_2 12 = 0.557\ldots$, proved in [15] and independently in [2].

In another line of research [20, 21, 9, 31], the finite field over which $f(X)$ is defined is assumed to be a prime field $\mathbb{F}_p$, and a *lifted polynomial* of $f(X)$ is assumed to be given, i.e., a degree-n polynomial $\tilde{f}(X) \in \mathbb{Z}[X]$ satisfying $\tilde{f}(X) \bmod p = f(X)$. In particular, Huang [20, 21] proved that $f(X) \in \mathbb{F}_p[X]$ can be deterministically factorized in polynomial time under GRH if the Galois group G of $\tilde{f}(X)$ is abelian. This was generalized in [9] to the case that G is solvable. For general G, Rónyai [31] gave a deterministic algorithm under GRH that runs in time polynomial in $|G|$ and the size of the input.

Recently, the author [18, 16, 17] proposed a unifying approach for deterministic polynomial factoring over finite fields based on the notion of *$\mathcal{P}$-schemes*, where $\mathcal{P}$ is a collection of subgroups of the Galois group G of $\tilde{f}(X)$. It was shown that above results [29, 10, 23, 20, 21, 9, 31] can be derived from this approach in a uniform way. In particular, the results based on m-schemes [23] may be obtained using $\mathcal{P}$-schemes by assuming G to be the full symmetric group $\mathrm{Sym}(n)$ (which is the most difficult case). When G is less complex than a full symmetric group, the approach based on $\mathcal{P}$-schemes may lead to better factoring algorithms by employing the structure of G. For example, a deterministic factoring algorithm was given in [18] (under GRH) whose running time is bounded in terms of the nonabelian composition factors of G. It runs in polynomial time when these nonabelian composition factors are all subquotients of $\mathrm{Sym}(k)$ for $k = 2^{O(\sqrt{\log n})}$.

1.1 Our Results.

This paper is a continuation of the work in [18, 16, 17]. We consider the problem of deterministically factoring $f(X) \in \mathbb{F}_p[X]$ given a lifted polynomial $\tilde{f}(X) \in \mathbb{Z}[X]$ of $f(X)$ whose Galois group is denoted by G. We want to apply the main result of [18] to families of Galois groups that are less complex than full symmetric groups. Natural candidates of such kinds of groups come from *linear groups*, which are the main focus of this paper.

For example, suppose the action of G on the set of n roots of $\tilde{f}(X)$ is permutation isomorphic to the action of $\mathrm{GL}(V)$ on $V \setminus \{0\}$, where V is a finite-dimensional vector space over a finite field $\mathbb{F}$. We know Evdokimov's algorithm [10] factorizes $f(X)$ in time $\mathrm{poly}(n^{\log n}, \log p)$, whereas Rónyai's algorithm [31] runs in time polynomial in $|\mathrm{GL}(V)| = n^{\Theta(\dim V)} = n^{\Theta(\log n/\log|\mathbb{F}|)}$ and the size of the input. When $|\mathbb{F}| = O(1)$, the latter time bound is still at least $\mathrm{poly}(n^{\log n}, \log p)$. Can we factorize $f(X)$ in time polynomial in $n^{o(\log n)}$ and the size of the input? We answer this question affirmatively in this paper.

Let S be a subset of a vector space V, and let G be a permutation group on S. We say *G acts linearly* on S if we can identify G with a subgroup of $\mathrm{GL}(V)$ such that the action of G on S is induced by the natural action of $\mathrm{GL}(V)$ on V. Our main result states as follows:

▶ **Theorem 1.** *Under GRH, there exists a deterministic algorithm that, given $f(X) \in \mathbb{F}_p[X]$ that factorizes into n distinct linear factors over $\mathbb{F}_p$, and a lifted polynomial $\tilde{f}(X) \in \mathbb{Z}[X]$ whose Galois group G acts linearly on the set S of roots of $\tilde{f}(X)$, where S is identified with a subset of a vector space V over a finite field $\mathbb{F}$, completely factorizes $f(X)$ over $\mathbb{F}_p$ in time polynomial in n^m and the size of the input, where m is an integer satisfying:*
(1) *$m = O(\log n)$ and $m \leq \dim\langle S\rangle_{\mathbb{F}}$, where $\langle S\rangle_{\mathbb{F}} \subseteq V$ is the subspace spanned by S over $\mathbb{F}$.*

(2) $m = O\left(\frac{\log n}{(\rho^2 \log\log\log\log n)^{1/3}}\right)$, *where* $\rho := \log|S|/\log|\langle S\rangle|$ *and* $\langle S\rangle \subseteq V$ *is the abelian subgroup generated by* S.

Note $\dim\langle S\rangle_{\mathbb{F}} = \frac{\log|S|}{\rho\log|\mathbb{F}|} = \frac{\log n}{\rho\log|\mathbb{F}|}$. Thus, the bound (2) slightly improves (1) when both ρ^{-1} and $|\mathbb{F}|$ are small enough.

▶ Remark. The assumption that $f(X)$ factorizes into distinct linear factors over $\mathbb{F}_p$ is not essential. It can be removed if we replace the $\mathcal{P}$-scheme algorithm [18] used in our proof by the generalized $\mathcal{P}$-scheme algorithm in [16, Chapter 5] which works for arbitrary f. We also note that there exists a standard reduction in literature that reduces the problem of factoring a univariate polynomial over a finite field to the special case of factoring a polynomial defined over a prime field $\mathbb{F}_p$ that factorizes into distinct linear factors over $\mathbb{F}_p$ [6, 39].

General Galois groups. Combining our techniques with [17], we also obtain an improved algorithm that applies to *any* finite Galois group G, whose running time is bounded in terms of the nonabelian composition factors of G.

Specifically, two functions $d_{\mathrm{Sym}}(m)$ and $d_{\mathrm{Lin}}(m,q)$ are introduced in [17]. These functions are further used to define quantities $N_{\mathcal{A}}(G) \in \mathbb{N}^+$ and $N_{\mathcal{C}}(G) \in \mathbb{N}^+$ respectively for every finite group G. The following theorem is then proved in [17].

▶ **Theorem 2** ([17, Theorem 1.2])**.** *Under GRH, there exists a deterministic algorithm that, given* $f(X) \in \mathbb{F}_p[X]$ *that factorizes into* n *distinct linear factors over* $\mathbb{F}_p$*, and a lifted polynomial* $\tilde{f}(X) \in \mathbb{Z}[X]$ *with Galois group* G*, completely factorizes* f *over* $\mathbb{F}_p$ *in time polynomial in* $N_{\mathcal{A}}(G)$*,* $N_{\mathcal{C}}(G)$*, and the size of the input.*

Here $N_{\mathcal{A}}(G)$ (resp. $N_{\mathcal{C}}(G)$) measures the contribution from the alternating groups (resp. classical groups) among the nonabelian composition factors of G to the running time. Using the bounds $d_{\mathrm{Sym}}(m) = O(\log m)$ and $d_{\mathrm{Lin}}(m,q) \le m$, it is shown in [17] that $N_{\mathcal{A}}(G), N_{\mathcal{C}}(G) = k^{O(\log k)}$ if these alternating groups and classical groups are all (isomorphic to) subquotients of a symmetric group $\mathrm{Sym}(k)$. In particular, choosing $k = n$ yields an $n^{O(\log n)}$-time deterministic algorithm under GRH, matching the state-of-the-art results [10, 23].

In this paper, we obtain the following new bound for $d_{\mathrm{Lin}}(m,q)$.

▶ **Theorem 3.** $d_{\mathrm{Lin}}(m,q) = O\left(\frac{m\log q}{(\log\log\log(m\log q))^{1/3}}\right)$.

This bound is derived from Theorem 5 stated below. Its proof is deferred to Appendix A, where the definition of $d_{\mathrm{Lin}}(m,q)$ is also given.

When q is small, the bound in Theorem 3 is better than the bound $d_{\mathrm{Lin}}(m,q) \le m$. It has the following implication, which states that the contribution $N_{\mathcal{C}}(G)$ from classical groups to the time complexity of the algorithm in Theorem 2 is always subpolynomial in $n^{\log n}$. Thus, the contribution $N_{\mathcal{A}}(G)$ from alternating groups is the only bottleneck for obtaining an $n^{o(\log n)}$-time deterministic algorithm under GRH.

▶ **Corollary 4.** *We have* $N_{\mathcal{C}}(G) = n^{o(\log n)}$ *in Theorem 2. Furthermore, if every alternating group among the composition factors of* G *has degree* $n^{o(1)}$*, then the algorithm in Theorem 2 runs in time polynomial in* $n^{o(\log n)}$ *and the size of the input.*

The proof of Corollary 4 is deferred to Appendix A.

Realizing a Galois group over $\mathbb{Q}$. Given the results above, it is a natural question to ask if a finite classical group G (or a finite group G that has large classical groups as composition factors) can indeed be realized as a Galois group over $\mathbb{Q}$. The problem of realizing a given group G as a Galois group over $\mathbb{Q}$ is known as the *inverse Galois problem* [26]. While this problem is unsolved in general, many partial results are known. In particular, there are infinite families of finite classical groups that are realizable over $\mathbb{Q}$. For example, $\mathrm{PSL}_n(p)$ is realizable over $\mathbb{Q}$ for odd prime p when $\gcd(n, p-1) = 1$, $p > 3$ and $p \not\equiv -1 \pmod{12}$ [26, Theorem III.6.8]. See [26, Section III.10.2] for a summary about realizing finite simple groups over $\mathbb{Q}$. These groups may also be used to build larger Galois groups via semidirect products or wreath products [26].

Furthermore, given a Galois extension $L/\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) = G$, we could realize any permutation representation $G \to \mathrm{Sym}(S)$ as follows: Let $H = G_x$ be a stabilizer for some $x \in S$, and let $K = L^H$, the fixed subfield of H. Choose $\tilde{f}(X) \in \mathbb{Z}[X]$ to be the minimal polynomial of an integral primitive element of K. Then the action of G on the set of roots of $\tilde{f}$ in L is permutation isomorphism to its action on S.

Finally, by Chebotarev's density theorem [27], there exist infinitely many primes p such that $\tilde{f}(X) \bmod p$ factorizes into distinct linear factors, so that Theorem 1 and Theorem 2 may apply.

1.2 Proof Overview

We give a high-level overview of the proof of Theorem 1 in this subsection.

Linear m-schemes. To prove Theorem 1, we introduce a family of combinatorial objects called *linear m-schemes*, which can be seen as the linear analogue of m-schemes studied in [23]. For $m \in \mathbb{N}^+$ and a subset $S \subseteq V$, a linear m-scheme on S is a collection $\Pi = \{\Pi^{(1)}, \ldots, \Pi^{(m)}\}$ of partitions satisfying a list of axioms, where $\Pi^{(i)}$ is a partition of S^i for $i \in [m]$ (see Definition 9 for the formal definition). We are interested in a special kind of linear m-schemes called *strongly antisymmetric linear m-schemes*. In particular, we will prove the following statement about these objects.

▶ **Theorem 5.** *Let V be a vector space over a finite field $\mathbb{F}$, $S \subseteq V$, $n = |S|$, and $\rho = \log|S| / \log|\langle S\rangle|$. Suppose Π is a strongly antisymmetric linear m-scheme on S, and $\Pi^{(1)}$ is* not *the finest partition of S. Then $m = O\left(\frac{\log n}{(\rho^2 \log\log\log\log n)^{1/3}}\right)$.*

Moreover, we relate linear m-schemes to the notion of $\mathcal{P}$-schemes in [18], which allows us to translate Theorem 5 into a statement about $\mathcal{P}$-schemes. Theorem 1 then follows from the machinery developed in [18]. As the general theory of $\mathcal{P}$-schemes is not the focus of this paper, we defer the derivation of Theorem 1 from Theorem 5 to the appendix (see Appendix A). The main text of this paper then focuses on Theorem 5, which is a purely combinatorial statement.

Reducing the cardinality of sets by restricting to a fiber. For $B \subseteq S$, $B' \subseteq B \times B$ and $x \in B$, call $B'_x := \{y \in S : (x, y) \in B'\} \subseteq B$ the *x-fiber* of B'. The combinatorics behind Evdokimov's algorithm [10] can be very roughly summarized as follows: The algorithm produces a partition P of the set S, such that if $B \in P$ is not a singleton, we can find $B' \subseteq B \times B$ and $x \in B$ such that $1 < |B'_x| < |B|/2$. The algorithm then replaces B by B'_x and repeats. At each step, $|B|$ is reduced by at least a factor of two. So this process has at most $\log|B| \le \log n$ steps, which gives the $O(\log n)$ upper bound for m. To prove the

inequality $|B'_x| < |B|/2$, Evdokimov crucially used the permutation $(\alpha, \beta) \mapsto (\beta, \alpha)$ of S^2, which can be seen as an element of the symmetric group $\mathrm{Sym}(2)$. The algorithm in [23] based on m-schemes then upgraded this method by using permutations in $\mathrm{Sym}(k)$ for $k \in [m]$.

Our analysis uses similar ideas. The main difference is that here the structure of linear Galois groups allows us to employ not only the permutations in $\mathrm{Sym}(k)$ but also *linear automorphisms*. For example, when $k = 2$, we will use not only the map $(\alpha, \beta) \mapsto (\beta, \alpha)$ but also maps of the form $(\alpha, \beta) \mapsto (a\alpha + b\beta, c\alpha + d\beta)$, where $a, b, c, d \in \mathbb{F}$. This set of permutations forms a permutation group larger than $\mathrm{Sym}(k)$. Because of the richer set of permutations, we are able to prove that on average, restricting to a fiber at each step reduces the cardinality of a set by a *superconstant* factor. This is summarized by Lemma 17 (the Key Lemma) from which the $o(\log n)$ bound in Theorem 5 follows.

Additive combinatorics. Our proof of Lemma 17 heavily uses tools from additive combinatorics. These tools seem very useful for studying linear m-schemes as they apply to "soft" combinatorial objects like subsets and partitions while also capturing the rigid abelian group structure of V. Specifically, our analysis for a subset $B \subseteq S$ is divided into the following three cases, depending on how large $B + B$ is compared with B and $B \times B$:

1. $|B| \ll |B + B| \ll |B|^2$. In this case, we show that if $K|B| \le |B + B| \le |B|^2/K$ for some factor K, then restricting to a fiber at each step reduces $|B|$ by a factor of $K^{\Omega(1)}$.
2. $|B+B|/|B|$ is small. This is the most difficult case and the proof becomes rather technical. In particular, we will prove a "decomposition theorem" using Fourier analysis. Due to the page limit, we defer the analysis for this case to the appendix.
3. $|B|^2/|B+B|$ is small. This happens only when the "entropy rate" $\rho(B) := \log|B|/\log|\langle B\rangle|$ is low ($\lessapprox 1/2$). We reduce this case to the previous two cases by replacing B with a partial sumset $B' \subseteq kB$ for some integer $k > 1$, which increases the entropy rate.

2 Notations and Preliminaries

Let $\mathbb{N} := \{0, 1, 2, \dots\}$ and $\mathbb{N}^+ := \{1, 2, \dots\}$. Let $[k] := \{1, 2, \dots, k\}$. Write log for base 2 logarithms. Denote by $A \setminus B$ the set difference $\{x : x \in A \text{ and } x \notin B\}$. The cardinality of a set S is $|S|$. Alternatively, we write $\#\{\cdots\}$ for the cardinality of a set $\{\cdots\}$. The restriction of a map $f : S \to S'$ to a subset $T \subseteq S$ is denoted by $f|_T$.

A *partition* of a set S is a set P of nonempty subsets of S satisfying $S = \coprod_{B\in P} B$, where $\coprod$ denotes the disjoint union. Each $B \in P$ is called a *block* of P. For $T \subseteq S$ and a partition P of S, the set $P|_T := \{B \cap T : B \in P\} \setminus \{\emptyset\}$ is a partition of T, called the *restriction* of P to T. Denote by ∞_S the finest partition of S, i.e., $\infty_S = \{\{x\} : x \in S\}$. For a set P of subsets of S, define $\mathcal{B}(P)$ to be the set of subsets of S that are unions of sets in P.

Additive combinatorics. Suppose V is a vector space over a field $\mathbb{F}$. For $A, B \subseteq V$, define $A + B := \{a + b : a \in A, b \in B\}$ and $A - B := \{a - b : a \in A, b \in B\}$. For $k \in \mathbb{N}^+$, write kA for $\underbrace{A + A + \cdots + A}_{k \text{ times}}$. Write $\langle A\rangle$ for the abelian subgroup of V generated by A. For $A, B \subseteq V$, define $\mu_B(A)$ to be the density of A in B, i.e., $\mu_B(A) := |A\cap B|/|B|$. Write $\mu(A)$ for $\mu_{\langle A\rangle}(A)$. Clearly, if $|\langle A\rangle|/|A|$ is small, so is $|A + A|/|A|$. The inverse of this fact is the content of the *Freiman–Ruzsa Theorem* [32]. We need the following version of this theorem.

▶ **Theorem 6** (Freiman–Ruzsa Theorem [11, 12]). *Let V be a vector space over a prime finite field $\mathbb{F}_\ell$. Suppose $A \subseteq V$ satisfies $|A + A| \le K|A|$ for some $K > 0$. Then $|\langle A\rangle| \le \ell^{2K}|A|$.*

We also need *Plünnecke's inequality*:

▶ **Theorem 7** (Plünnecke's inequality [37, Corollary 6.28]). *Suppose $A, B \subseteq V$ satisfies $|A+B| \leq K|A|$ for some $K > 0$. Then $|kB| \leq K^k|A|$ for $k \in \mathbb{N}^+$.*

3 Introducing Linear m-schemes

Let V be a finite-dimensional vector space over a finite field $\mathbb{F}$. For $k, k' \in \mathbb{N}^+$, denote by $\mathcal{M}_{k,k'}(\mathbb{F})$ the set of linear maps $\tau : V^k \to V^{k'}$ of the form

$$\mathbf{x} = (x_1, \ldots, x_k) \mapsto \left(\sum_{i=1}^{k} c_{i,1} x_i, \ldots, \sum_{i=1}^{k} c_{i,k'} x_i \right), \quad \text{where } c_{i,j} \in \mathbb{F},$$

i.e., each coordinate of $\tau(\mathbf{x}) \in V^{k'}$ is a linear combination of the coordinates of $\mathbf{x} \in V^k$ over $\mathbb{F}$. In most cases, the base field $\mathbb{F}$ is clear from the context and we simply write $\mathcal{M}_{k,k'}$ for $\mathcal{M}_{k,k'}(\mathbb{F})$.

The following special maps in $\mathcal{M}_{k,1}$ will be used in the paper.

▶ **Definition 8** (projection and summation). *For $k \in \mathbb{N}^+$ and $i \in [k]$, write $\pi_{k,i} : V^k \to V$ for the projection of V^k to its ith coordinate, and write $\sigma_k : V^k \to V$ for the map sending $(x_1, \ldots, x_k) \in V^k$ to $x_1 + x_2 + \cdots + x_k$. We have $\pi_{k,i}, \sigma_k \in \mathcal{M}_{k,1}$ for $k \in \mathbb{N}^+$ and $i \in [k]$.*

Now we are ready to define the notion of *linear m-schemes*.

▶ **Definition 9** (linear m-scheme). *Let $m \in \mathbb{N}^+$ and $S \subseteq V$. Let $\Pi = \{\Pi^{(1)}, \ldots, \Pi^{(m)}\}$, where $\Pi^{(k)}$ is a partition of S^k for $k \in [m]$. We say Π is a* linear m-scheme *on S if for $k, k' \in [m]$, $B \in \Pi^{(k)}$, $B' \in \Pi^{(k')}$, and $\tau \in \mathcal{M}_{k,k'}$, we have*
(P1): *Either $\tau(B) = B'$ or $\tau(B) \cap B' = \emptyset$.*
(P2): *$\#\{x \in B : \tau(x) = y\}$ is constant when y ranges over B'.*

Definition 9 can be viewed as a linear analogue of m-schemes in [23]. In fact, it is not hard to show that a linear m-scheme on a set S always induces an m-scheme on S.

The following lemma states that the coordinates of elements in the same block of a linear m-scheme always satisfy the same linear relations. Its proof can be found in the appendix.

▶ **Lemma 10.** *Let Π be a linear m-scheme on S. For $k \in [m]$, $B \in \Pi^{(k)}$ and $\mathbf{x} = (x_1, \ldots, x_k), \mathbf{y} = (y_1, \ldots, y_k) \in B$, the coordinates x_i satisfy a linear relation $\sum_{i=1}^{k} c_i x_i = 0$ iff the coordinates y_i satisfy the same relation, i.e., $\sum_{i=1}^{k} c_i y_i = 0$.*

Strong antisymmetry. We are interested in a special kind of linear m-schemes called *strongly antisymmetric linear m-schemes*.

▶ **Definition 11** (strong antisymmetry). *Let Π be a linear m-scheme. Define*

$$\mathcal{M}_\Pi := \left\{ \tau|_B : B \to B' \;\middle|\; \begin{array}{l} k, k' \in [m], B \in \Pi^{(k)}, B' \in \Pi^{(k')}, \\ \tau \in \mathcal{M}_{k,k'}, \tau \text{ maps } B \text{ bijectively to } B' \end{array} \right\}.$$

Define $\widetilde{\mathcal{M}}_\Pi$ to be the set of all possible compositions of the maps $\tau \in \mathcal{M}_\Pi$ as well as their inverses τ^{-1}. We say Π is strongly antisymmetric *if for $k \in [m]$ and $B \in \Pi^{(k)}$, $\widetilde{\mathcal{M}}_\Pi$ does not contain a nontrivial permutation of B.*

3.1 Basic Facts about Linear m-schemes

In this subsection, we list some basic facts about linear m-schemes. Most proofs are omitted due to the page limit and can be found in the appendix.

Closedness of sets $\mathcal{B}(\Pi^{(k)})$. Recall that for a set P of subsets of S, we define $\mathcal{B}(P)$ to be the set of subsets of S that are unions of sets in P. The following lemma states that for a linear m-scheme Π, the sets $\mathcal{B}(\Pi^{(k)})$ are closed under various operations.

▶ **Lemma 12.** *Let Π be a linear m-scheme on $S \subseteq V$. We have:*
1. *For $k \in [m]$, $\mathcal{B}(\Pi^{(k)})$ is closed under union, intersection, and complement in S^k.*
2. *Let $k, k' \in [m]$ such that $k + k' \le m$. Let $B \in \mathcal{B}(\Pi^{(k+k')})$. Let Q be a quantifier of the form $\exists$, $\forall$, or $\exists_{=t}$ (which means "there exist exactly t elements"). Let B_Q be the set of $x \in S^k$ satisfying the condition "$Q\, y \in S^{k'} : (x, y) \in B$". Then $B_Q \in \mathcal{B}(\Pi^{(k)})$.*
3. *Let $k, k' \in [m]$, $B \in \mathcal{B}(\Pi^{(k)})$, and $\tau \in \mathcal{M}_{k,k'}$. Then $\tau(B) \cap S^{k'} \in \mathcal{B}(\Pi^{(k')})$.*
4. *Let $k, k' \in [m]$, $B \in \mathcal{B}(\Pi^{(k')})$, and $\tau \in \mathcal{M}_{k,k'}$. Then $\tau^{-1}(B) \cap S^k \in \mathcal{B}(\Pi^{(k)})$.*

Recursive structure of linear m-schemes. Next, we show that linear m-schemes have a recursive structure. Namely, for $t \in [m-1]$, each "fiber" of a linear m-scheme with respect to the projection to the first t coordinates is a linear $(m-t)$-scheme.

▶ **Definition 13.** *Let Π be a linear m-scheme on $S \subseteq V$. Let $t \in [m-1]$ and $x = (x_1, \ldots, x_t) \in S^t$. Define $\Pi_x = \left\{\Pi_x^{(1)}, \ldots, \Pi_x^{(m-t)}\right\}$, where for $k \in [m-t]$, $\Pi_x^{(k)}$ is the partition of S^k such that two elements $y, z \in S^k$ are in the same block of $\Pi_x^{(k)}$ iff $(x, y), (x, z) \in S^{t+k}$ are in the same block of $\Pi^{(t+k)}$. Also write $\Pi_{x_1,\ldots,x_t}$ for Π_x.*

▶ **Lemma 14.** *Π_x in Definition 13 is a linear $(m-t)$-scheme on S. Moreover, if Π is strongly antisymmetric, so is Π_x.*

We also have the following easy observation.

▶ **Lemma 15.** *Let Π and Π_x be as in Definition 13. Then $\mathcal{B}(\Pi^{(1)}) \subseteq \mathcal{B}(\Pi_x^{(1)})$, i.e., the partition $\Pi_x^{(1)}$ refines $\Pi^{(1)}$.*

Proof. As $\Pi_{x_1,\ldots,x_t} = (\Pi_{x_1,\ldots,x_{t-1}})_{x_t}$, it suffices to prove the claim for $t = 1$. The claim follows by noting that $B \times B \in \mathcal{B}(\Pi^{(2)})$ for $B \in \mathcal{B}(\Pi^{(1)})$. ◀

Basic upper bounds for m. Next, we give the following basic upper bounds for m when Π is a strongly antisymmetric linear m-scheme satisfying $\Pi^{(1)} \neq \infty_S$.

▶ **Lemma 16.** *Suppose Π is a strongly antisymmetric linear m-scheme on $S \subseteq V$, where $|S| = n$, and $B \in \Pi^{(1)}$ is not a singleton. Denote by $\langle S \rangle_{\mathbb{F}}$ the subspace of V spanned by S over $\mathbb{F}$. Then (1) $m < \dim\langle S \rangle_{\mathbb{F}}$ and (2) $m \le \log |B| \le \log n$.*

4 Proof of Theorem 5

In the rest of the paper, Π is assumed to be a strongly antisymmetric linear m-scheme on $S \subseteq V$, where V is a finite-dimensional vector space over a finite field $\mathbb{F}$. Let $n := |S|$, $\rho := \log |S| / \log |\langle S \rangle|$, and $\ell := \mathrm{char}(\mathbb{F})$.

Assumptions. Throughout the analysis, we make the following assumptions: Assume $n \ge C$ for some sufficiently large constant C. Also assume $\rho^2 \log\log\log\log n > 1$, since otherwise Theorem 5 holds by Lemma 16 (2).

In addition, we assume $\mathbb{F}$ is a *prime field*, which can be justified as follows: Note that V, as a vector space over $\mathbb{F}$, may be identified with a vector space over $\mathbb{F}_\ell$. Under this identification, we have $\mathcal{M}_{k,k'}(\mathbb{F}_\ell) \subseteq \mathcal{M}_{k,k'}(\mathbb{F})$ for $k, k' \in [m]$, because linear combinations of

the k coordinates of $\mathbf{x} \in V^k$ over $\mathbb{F}_\ell$ are also linear combinations of these coordinates over $\mathbb{F}$. This means if Π is a strongly antisymmetric linear m-scheme over $\mathbb{F}$, then it remains so over $\mathbb{F}_\ell$. Therefore, it suffices to prove Theorem 5 for the case $\mathbb{F} = \mathbb{F}_\ell$.

Because of the assumption that $\mathbb{F}$ is a prime field, the abelian group $\langle S \rangle$ and the $\mathbb{F}$-subspace $\langle S \rangle_{\mathbb{F}}$ spanned by S coincide. They are used interchangeably from now on.

Finally, assume $\log \ell \le (\rho^{-1} \log\log\log\log n)^{1/3} \le (\log\log\log\log n)^{1/2}$, since otherwise $\dim \langle S \rangle_{\mathbb{F}} = \log_\ell n^{1/\rho} \le \frac{\log n}{(\rho^2 \log\log\log\log n)^{1/3}}$ and Theorem 5 holds by Lemma 16 (1).

Reduction to the Key Lemma. The following lemma is the key in the proof of Theorem 5.

▶ **Lemma 17** (Key Lemma). *Suppose $B \in \Pi^{(1)}$ has cardinality at least $n^{1/(\rho^2 \log\log\log\log n)^{1/3}}$, and $m \ge (\log\log n)^2$. Then there exist $k \in [m-2]$, $x_1, \dots, x_k \in B$, and $B' \in \mathcal{B}(\Pi^{(1)}_{x_1,\dots,x_k})$ such that $B' \subseteq B$ and $\min\{|B'|, |B|/|B'|\} \ge 2^{Ck(\rho^2 \log\log\log\log n)^{1/3}}$ for some constant $C > 0$.*

We first use Lemma 17 to prove a very similar lemma below, which shows that on average, replacing Π by Π_x at each step reduces the cardinality of blocks by a superconstant factor.

▶ **Lemma 18.** *Suppose $B \in \Pi^{(1)}$, $|B| \ge n^{1/(\rho^2 \log\log\log\log n)^{1/3}} > 1$, and $m \ge (\log\log n)^2$. Then there exist $k \in [m-2]$, $x_1, \dots, x_k \in B$, and $B' \in \Pi^{(1)}_{x_1,\dots,x_k}$ such that $B' \subsetneq B$, $|B'| > 1$, and $|B|/|B'| \ge 2^{Ck(\rho^2 \log\log\log\log n)^{1/3}}$ for some constant $C > 0$.*

Due to the page limit, we omit the derivation of Lemma 18 from Lemma 17 and defer it to the appendix. Theorem 5 now follows from Lemma 18 and a simple induction:

Proof of Theorem 5. If $m < (\log\log n)^2$ then we are done. So assume $m \ge (\log\log n)^2$. Let $C > 0$ be the constant in Lemma 18. Let $t := 1/(\rho^2 \log\log\log\log n)^{1/3}$. Choose $B \in \Pi^{(1)}$ such that $|B| > 1$. We claim

$$m \le C^{-1} t \log |B| + t \log n = O\left(\frac{\log n}{(\rho^2 \log\log\log\log n)^{1/3}}\right).$$

Induct on $|B|$. If $|B| < n^t$, we have $m \le \log |B| \le t \log n$ by Lemma 16 (2). So the claim holds in this case. Now assume $|B| \ge n^t$. Then we can choose $k \in [m-2]$, $x_1, \dots, x_k \in B$, and $B' \in \Pi^{(1)}_{x_1,\dots,x_k}$ as in Lemma 18. By Lemma 14, $\Pi_{x_1,\dots,x_k}$ is a strongly antisymmetric $(m-k)$-scheme. By the induction hypothesis, we have $m - k \le C^{-1} t \log |B'| + t \log n$. The claim then follows from the inequality $|B'| \le 2^{-Ck/t} |B|$. ◀

So it remains to prove Lemma 17. We divide its proof into three cases: (1) $|B| \ll |B+B| \ll |B|^2$, (2) $|B+B|/|B|$ is small, and (3) $|B|^2/|B+B|$ is small.

4.1 The Case $|B| \ll |B+B| \ll |B|^2$

We first prove Lemma 17 for the case $|B| \ll |B+B| \ll |B|^2$. To see the intuition, consider $x, y \in B$. The set $B \cap (x+y-B) = \{z \in B : x+y-z \in B\}$ is in $\mathcal{B}(\Pi^{(1)}_{x,y})$, since $\{(x,y,z) \in S^3 : z \in B, x+y-z \in B\} \in \mathcal{B}(\Pi^{(3)})$ by Lemma 12 (1) and (4). Moreover, $B \cap (x+y-B)$ maps bijectively to $\{(z,w) \in B \times B : z+w = x+y\}$ via $z \mapsto (z, x+y-z)$. Therefore,

$$|B \cap (x+y-B)| = \#\{(z,w) \in B \times B : z+w = x+y\}.$$

On the other hand, we have

$$\sum_{t \in B+B} \#\{(z,w) \in B \times B : z+w = t\} = |B \times B| = |B|^2.$$

Let us pretend that the sets $\{(z,w) \in B \times B : z+w=t\}$ have equal size for all $t \in B+B$. Then we may choose $B' = B \cap (x+y-B)$ for arbitrary $x, y \in B$, whose cardinality is $|B'| = |B|^2/|B+B|$. As $|B| \ll |B+B| \ll |B|^2$, both $|B'|$ and $|B|/|B'|$ are large, as required by Lemma 17.

In general, the sets $\{(z,w) \in B \times B : z+w=t\}$ may have very different sizes. Still, we manage to prove that if $K|B| \le |B+B| \le |B|^2/K$ holds for some $K \ge 4$, then there exist $x, y \in B$ and a subset B' of B in $\mathcal{B}(\Pi^{(1)}_{x,y})$ such that $|B'|, |B|/|B'| \ge K^{1/2}$. In fact, in order to later extend the analysis to the case that $|B|^2/|B+B|$ is small, we prove the result in the following more general form.

▶ **Lemma 19.** *Let $B \in \Pi^{(1)}$ and $k \in \mathbb{N}^+$. Suppose $m \ge 2k+2$. Let A be a block in $\Pi^{(k)}$ contained in B^k, and let $A' = \sigma_k(A)$ (see Definition 8). Suppose $K|A'| \le |A'+B| \le |A'||B|/K$ for some $K \ge 4$. Then there exist $x_1, \dots, x_{k+1} \in B$ and $B' \in \mathcal{B}(\Pi^{(1)}_{x_1,\dots,x_{k+1}})$ such that $B' \subseteq B$ and $\min\{|B'|, |B|/|B'|\} \ge K^{1/2}$.*

In particular, by choosing $k=1$ and $A = A' = B$, we see that Lemma 17 holds when $K|B| \le |B+B| \le |B|^2/K$ for some $K = 2^{\Omega((\rho^2 \log\log\log n)^{1/3})} \ge 4$.

Proof of Lemma 19. For $z \in A'+B$, define $\nu^+(z) := \#\{(x,y) \in A' \times B : x+y=z\}$. First assume there exists an element $z \in A'+B$ such that $\nu^+(z) \in [K^{1/2}, |B|/K^{1/2}]$. Fix such z. Choose $(x_1, \dots, x_k) \in A$ and $x_{k+1} \in B$ such that $x_1 + \cdots + x_{k+1} = z$. Let $T = \{y \in B : z-y \in A'\}$. Note $y \mapsto (z-y, y)$ is a one-to-one correspondence between T and $\{(x,y) \in A' \times B : x+y=z\}$. So $|T| = \nu^+(z) \in [K^{1/2}, |B|/K^{1/2}]$. We also have

$$T = \{y \in B : \exists\, (x'_1, \dots, x'_k) \in A : x'_1 + \cdots + x'_k + y = x_1 + \cdots + x_{k+1}\}$$

which is in $\mathcal{B}(\Pi^{(1)}_{x_1,\dots,x_{k+1}})$ by Lemma 12. Choosing $B' = T$ proves the lemma.

So we may assume $\nu^+(z) \notin [K^{1/2}, |B|/K^{1/2}]$ for $z \in A'+B$. Define

$$Z := \{z \in A'+B : \nu^+(z) \le |B|/K^{1/2}\} = \{z \in A'+B : \nu^+(z) < K^{1/2}\}.$$

As $\sum_{z \in A'+B} \nu^+(z) = |A'||B|$, the number of $z \in A'+B$ satisfying $\nu^+(z) > |B|/K^{1/2}$ is less than $K^{1/2}|A'|$. So we have

$$|Z| > |A'+B| - K^{1/2}|A'| \ge K|A'| - K^{1/2}|A'| \ge K^{1/2}|A'|$$

where the last inequality holds since $K \ge 4$.

For $x \in A'$, define $Z_x := \{y \in B : x+y \in Z\}$. Then $Z = \bigcup_{x \in A'}(x + Z_x)$. Therefore,

$$\sum_{x \in A'} |Z_x| \ge |Z| \ge K^{1/2}|A'|. \tag{1}$$

On the other hand, we have

$$\begin{aligned} \sum_{x \in A'} |Z_x| &= \#\{(x,y) \in A' \times B : x+y \in Z\} = \sum_{z \in Z} \#\{(x,y) \in A' \times B : x+y=z\} \\ &= \sum_{z \in Z} \nu^+(z) \le K^{1/2}|A'+B| \le |A'||B|/K^{1/2}. \end{aligned} \tag{2}$$

▷ Claim 20. $|Z_x|$ is constant when x ranges over A'.

Proof of Claim 20. For $t \in \mathbb{N}$, let A_t be the set of $y \in A$ such that there exist precisely t elements $x \in A$ satisfying $\sigma_k(x) = \sigma_k(y)$. Then $A_t \in \mathcal{B}(\Pi^{(k)})$ for $t \in \mathbb{N}$ by Lemma 12. Also

note $A = \bigcup_{t\in\mathbb{N}} A_t$. As $A \in \Pi^{(k)}$, we have $A = A_{t_0}$ for some $t_0 \in \mathbb{N}$. This means for all $z \in A'$, there exist precisely t_0 elements $x \in A$ satisfying $\sigma_k(x) = z$.

For $t \in \mathbb{N}$, denote by X_t the set of $(z, w) \in A \times B$ such that there exist precisely t elements $(x, y) \in A' \times B$ satisfying $x + y = \sigma_k(z) + w$, or equivalently, there exist precisely tt_0 elements $(x, y) \in A \times B$ satisfying $\sigma_k(x) + y = \sigma_k(z) + w$. The latter characterization shows $X_t \in \mathcal{B}(\Pi^{(k+1)})$ for $t \in \mathbb{N}$ by Lemma 12. Let $Z' = \bigcup_{t\in\mathbb{N}:t<K^{1/2}} X_t \in \mathcal{B}(\Pi^{(k+1)})$. Then $(x, y) \in A \times B$ is in Z' iff $\sigma_k(x) + y$ is in Z.

For $t \in \mathbb{N}$, denote by Y_t the set of $x \in A$ such that there exist precisely t elements $y \in B$ satisfying $(x, y) \in Z'$, or equivalently, $\sigma_k(x) + y \in Z$. We have $Y_t \in \mathcal{B}(\Pi^{(k)})$ for $t \in \mathbb{N}$ by Lemma 12. Also note $A = \bigcup_{t\in\mathbb{N}} Y_t$. As $A \in \Pi^{(k)}$, we have $A = Y_{t_1}$ for some $t_1 \in \mathbb{N}$. So for all $x \in A$, there exist precisely t_1 elements $y \in B$ such that $\sigma_k(x) + y \in Z$, i.e., $|Z_{\sigma_k(x)}| = t_1$. As $A' = \sigma_k(A)$, this proves the claim. ◁

By (1), (2) and Claim 20, we have $K^{1/2} \le |Z_x| \le |B|/K^{1/2}$ for all $x \in A'$. Choose arbitrary $x = (x_1, \ldots, x_k) \in A$ and $x_{k+1} \in B$, and let $x' = \sigma_k(x) \in A'$. Note $Z_{x'} = \{y \in B : x' + y \in Z\} = \{y \in B : (x, y) \in Z'\}$ is in $\mathcal{B}(\Pi^{(1)}_{x_1,\ldots,x_k}) \subseteq \mathcal{B}(\Pi^{(1)}_{x_1,\ldots,x_k,x_{k+1}})$. The lemma follows by choosing $B' = Z_{x'}$. ◀

4.2 The Case $|B + B|/|B|$ is small

Next, we address the case that $|B+B|/|B|$ is small. This is equivalent to $\mu(B)^{-1} = |\langle B\rangle|/|B|$ being small by the Freiman-Ruzsa Theorem (Theorem 6). Our main result in this case is the following lemma.

▶ **Lemma 21.** *Let $N \ge c$ such that $\log \ell \le (\log\log\log\log N)^{1/2}$, where $c > 0$ is a sufficiently large constant. Suppose $B \in \Pi^{(1)}$, $|B + B|/|B| \le (\log\log\log N)^{1/2}$, and $m, |B| \ge \log\log N$. Then there exist $k = O(\log\log\log N)$, $x_1, \ldots, x_k \in B$, and $B' \in \mathcal{B}(\Pi^{(1)}_{x_1,\ldots,x_k})$ such that $B' \subseteq B$ and $2^{Ck\log\log\log\log N} \le |B|/|B'| \le 2^{(\log N)^{1/2}}$ for some constant $C > 0$.*

Due to the page limit, we defer the proof of Lemma 21 to the appendix (see Appendix D). Here we only sketch the main ideas: Observe that the argument in Subsection 4.1 does not directly apply since B is dense in $\langle B\rangle$ and therefore $|B + B|/|B|$ is small. So our first step is reducing the density of B. Roughly speaking, we show that restricting to a fiber of Π (i.e., replacing Π by Π_x for some $x \in B$) each time reduces not only the cardinality of a block but also its *density* by at least a constant factor. By repeatedly restricting to fibers k times for some $k = \omega(1)$, we reduce the density of a block to $\exp(-k)$. Then we manage to prove Lemma 21 by repeatedly applying an argument similar to that in Subsection 4.1 to blocks that are already sparse enough.

The actual proof is much more complicated than the above sketch due to many technical issues that we need to solve, and we refer the reader to the appendix for the full details. For example, one issue is that replacing $B \in \Pi^{(1)}$ by a subset $B' \in \Pi^{(1)}_x$, while always reducing the cardinality, may actually increase the density (i.e., $\mu(B') > \mu(B)$). We observe that this happens only when B is "overrepresented" in the subspace $\langle B'\rangle$. To solve this problem, we find a small collection of subspaces $W_i \subseteq \langle B\rangle$ such that B becomes "pseudorandom" within each W_i, which ensures that overrepresentation never occurs within W_i. We state this as the *decomposition theorem* (Theorem 40). The actual proof of Lemma 21 then uses the density $\mu_{W_i}(B)$ of B in some W_i instead of $\mu(B)$.

4.3 The Case $|B|^2/|B+B|$ is small

Finally, we address the case that $|B|^2/|B+B|$ is small and finish the proof of Lemma 17. When $|B|^2/|B+B|$ is small, the argument in Subsection 4.1 does not directly apply since there are not enough linear dependencies of the form $a+b=c+d$ with $a,b,c,d \in B$. To solve this problem, we first find a partial sumset $A' = \sigma_k(A)$ for some $A \subseteq B^k$, where $k \in \mathbb{N}^+$ is small, such that either $|A'+A'|/|A'|$ is small or Lemma 17 already holds.

For $B \subseteq V$, define $\rho(B) := \log|B|/\log|\langle B\rangle|$. Then we have

▶ **Lemma 22.** *Let $K \geq 4$. Suppose $B \in \Pi^{(1)}$ has cardinality at least $2K^2$ and $m > 4/\rho(B) + \log K + 1$. Then one of the following is true:*

1. *There exist $1 \leq k \leq 2/\rho(B)+1$, $x_1,\dots,x_k \in B$, and $B' \in \mathcal{B}(\Pi^{(1)}_{x_1,\dots,x_k})$ such that $B' \subseteq B$ and $\min\{|B'|, |B|/|B'|\} \geq K^{1/2}$.*
2. *There exist $1 \leq k \leq 2/\rho(B)$ and $A \in \Pi^{(k)}$ such that $A \subseteq B^k$, $|A| \geq |B|^k/K^{(k-1)/2}$, $|A'+A'| \leq K^{2k}|A'|$, and $\sigma_k|_A : A \to A'$ is bijective, where $A' := \sigma_k(A)$.*

The proof of Lemma 22 uses the following lemma, whose proof is deferred to the appendix.

▶ **Lemma 23.** *Let $k \in [m]$, $A \in \Pi^{(k)}$ and $A' = \sigma_k(A)$. Suppose $m \geq 2k$ and $m > k + \log(|A|/|A'|)$. Then σ_k maps A bijectively to A'. In particular, $|A'| = |A|$.*

Proof of Lemma 22. Let $k=1$ and $A = A' = B$. We will gradually increase k and update $A, A' = \sigma_k(A)$ until we find the desired data. Throughout the process, we maintain the invariants that $A \subseteq B^k$, $|A| \geq |B|^k/K^{(k-1)/2}$ and $\sigma_k|_A : A \to A'$ is bijective, which obviously hold when $k=1$. Note these invariants imply $k \leq 2/\rho(B)$ since $|A| = |A'| \leq |\sigma_k(B^k)| \leq |\langle B\rangle|$ and $|A| \geq |B|^k/K^{(k-1)/2} \geq |B|^{k/2}$.

Consider the following cases.

Case 1: $K|A'| \leq |A'+B| \leq |A'||B|/K$**.** In this case, (1) of the lemma holds by Lemma 19.

Case 2: $|A'+B| < K|A'|$**.** It follows from Plünnecke's inequality (Theorem 7) that $|2kB| \leq K^{2k}|A'|$. As $A'+A' \subseteq 2kB$, we have $|A'+A'| \leq K^{2k}|A'|$. So (2) holds.

Case 3: $|A'+B| > |A'||B|/K$**.** In this case, let T be the union of the blocks $B' \in \Pi^{(k+1)}$ satisfying $B' \subseteq A \times B$ and $|B'| \leq K^{1/2}|A|$. First assume $|T| \geq K^{1/2}|A|$. By removing a subset of blocks in $\Pi^{(k+1)}$ from T if necessary, we can find a subset $T' \subseteq T$ such that $T' \in \mathcal{B}(\Pi^{(k+1)})$ and $K^{1/2}|A| \leq |T'| \leq 2K^{1/2}|A| \leq |A||B|/K^{1/2}$. Choose $x \in A$ and let $B' = \{y \in B : (x,y) \in T'\} \in \mathcal{B}(\Pi^{(1)}_x)$. Then $|B'| = |T'|/|A| \in [K^{1/2}, |B|/K^{1/2}]$ by Property (P2). So (1) holds.

So we may assume $|T| < K^{1/2}|A|$. For $x \in A$, the number of $y \in B$ satisfying $(x,y) \in T$ is bounded by $K^{1/2}$ by Property (P2). So $|\sigma_{k+1}(T)| \leq K^{1/2}|A'|$. Let $U = (A \times B) \setminus T$. As $A'+B = \sigma_{k+1}(A \times B) = \sigma_{k+1}(T) \cup \sigma_{k+1}(U)$, we have

$$|\sigma_{k+1}(U)| \geq |A'+B| - |\sigma_{k+1}(T)| \geq |A'||B|/K - K^{1/2}|A'| \geq |A'||B|/(2K).$$

So $|U| \leq |A \times B| = |A'||B| \leq 2K|\sigma_{k+1}(U)|$. By an averaging argument, there exists $A^* \in \Pi^{(k+1)}$ such that $A^* \subseteq U$ and $|A^*| \leq 2K|\sigma_{k+1}(A^*)|$. By Lemma 23 and the fact $m \geq 4/\rho(B) + \log K + 1$, the map $\sigma_{k+1}|_{A^*} : A^* \to \sigma_{k+1}(A^*)$ is bijective. Pick $x \in A$ and let $B' = \{y \in B : (x,y) \in A^*\}$. Then $B' \in \Pi^{(1)}_x$. As $A^* \subseteq U$, we have $|B'| = |A^*|/|A| \geq K^{1/2}$. If $|B'| \leq |B|/K^{1/2}$ then (1) holds. So assume $|B'| > |B|/K^{1/2}$. Then $|A^*| = |A||B'| \geq |A||B|/K^{1/2} \geq |B|^{k+1}/K^{k/2}$, where the last inequality holds since $|A| \geq |B|^k/K^{(k-1)/2}$.

Then we replace k, A, and A' by $k+1$, A^*, and $\sigma_{k+1}(A^*)$ respectively. Note all the invariants are preserved.

Continue the above process and note k never exceeds $2/\rho(B)$. This proves the lemma. ◀

In Case (2) of Lemma 22, we obtain a set $A' = \sigma_k(A)$ such that $|A' + A'|/|A'|$ is small. Our strategy in this case consists of the following steps:

1. Using Π to construct a new linear m'-scheme Π' on A' such that $A' \in \Pi'^{(1)}$, where $m' \le m$.
2. Applying Lemma 21 to Π' and A', and obtain an improved bound with respect to Π'.
3. Turning the bound obtained in Step (2) into an improved bound with respect to Π.

Step (1) is achieved by the following lemma, whose proof is deferred to the appendix.

▶ **Lemma 24.** *Let $k, m' \in [m]$, $A \in \Pi^{(k)}$ and $A' = \sigma_k(A)$ such that $m \ge 2km'$ and $\sigma_k|_A : A \to A'$ is bijective. For $k \in [m']$, write $\sigma_k^{(i)} : V^{ki} \to V^i$ for the map sending $(x_1, \dots, x_i)$ to $(\sigma_k(x_1), \dots, \sigma_k(x_i))$, where $x_1, \dots, x_i \in V^k$. Define $\Pi' = \{\Pi'^{(1)}, \dots, \Pi'^{(m')}\}$ such that for $i \in [m']$, $\Pi'^{(i)} := \{\sigma_k^{(i)}(B) : B \in \Pi^{(ki)}, B \subseteq A^i\}$. Then Π' is a well defined strongly antisymmetric linear m'-scheme on A'. Moreover, for $i \in [m']$ and $B \in \Pi^{(ki)}$ satisfying $B \subseteq A^i$, the map $\sigma_k^{(i)}|_B : B \to \sigma_k^{(i)}(B)$ is bijective.*

Now we are ready to prove Lemma 17.

Proof of Lemma 17. As $|\langle B\rangle| \le |\langle S\rangle| = |S|^{1/\rho} = n^{1/\rho}$ and $|B| \ge n^{1/(\rho^2 \log\log\log\log n)^{1/3}}$, we have $\rho(B) = \log|B|/\log|\langle B\rangle| \ge (\rho/\log\log\log\log n)^{1/3}$. Let $K = (\log\log\log n)^{\rho(B)/8}$. By Lemma 22, one of the following is true:

1. There exist $1 \le k \le 2/\rho(B)+1$, $x_1, \dots, x_k \in B$, and $B' \in \mathcal{B}(\Pi^{(1)}_{x_1,\dots,x_k})$ such that $B' \subseteq B$ and $\min\{|B'|, |B|/|B'|\} \ge K^{1/2}$.
2. There exist $1 \le k \le 2/\rho(B)$ and $A \in \Pi^{(k)}$ such that $A \subseteq B^k$, $|A| \ge |B|^k/K^{(k-1)/2}$, $|A' + A'| \le K^{2k}|A'|$, and $\sigma_k|_A : A \to A'$ is bijective, where $A' := \sigma_k(A)$.

If (1) holds then we are done since $K^{1/2} = 2^{\Omega(\rho(B)\log\log\log\log n)} = 2^{\Omega(k(\rho^2\log\log\log\log n)^{1/3})}$. So assume (2) holds. Choose $m' = \lfloor m/(2k)\rfloor$. Let Π' be the strongly antisymmetric linear m'-scheme on A' constructed from Π as in Lemma 24.

As $|A' + A'| \le K^{2k}|A'|$ and $K^{2k} \le K^{4/\rho(B)} \le (\log\log\log n)^{1/2}$, we know by Lemma 21 (applied to Π', A', and $N = n$) that there exist $r = O(\log\log\log n)$, $x_1, \dots, x_r \in A'$, and $A'' \in \mathcal{B}(\Pi'^{(1)}_{x_1,\dots,x_r})$ such that $A'' \subseteq A'$ and

$$2^{Cr\log\log\log\log n} \le |A'|/|A''| \le 2^{(\log n)^{1/2}}$$

for some constant $C > 0$.

For $i \in [r]$, choose $y_i \in A$ such that $\sigma_k(y_i) = x_i$. Let $y = (y_1, \dots, y_r) \in A^r \subseteq B^{kr}$. We then have the following claim, whose proof is deferred to the appendix.

▷ Claim 25. There exists a set $T \in \mathcal{B}(\Pi^{(k)}_y)$ such that $T \subseteq A$ and $|T| = |A''|$.

Let T be as in Claim 25. Let $K' = (\log\log\log n)^{r\rho(B)}$. For $0 \le i \le k$, let $\pi_i : V^k \to V^i$ be the projection to the first i coordinates. For $i \in [k]$, we say a block $U \in \Pi^{(k)}_y$ is *i-small* if $|\pi_i(U)|/|\pi_{i-1}(U)| \le K'$. For $i \in [k]$, let T_i be the union of the i-small blocks $U \in \mathcal{B}(\Pi^{(k)}_y)$ satisfying $U \subseteq T$. We address the following two cases separately:

Case 1: $|T_i| \geq K'|B|^{k-1}$ **for some** $i \in [k]$**.** Fix such $i \in [k]$. As $T_i \subseteq T \subseteq A \subseteq B^k$, we have $|\pi_{i-1}(T_i)| \leq |B|^{i-1}$ and $|\pi_i(T_i)| \geq |T_i|/|B|^{n-i} \geq K'|B|^{i-1}$. By the pigeonhole principle, there exists $z \in \pi_{i-1}(T_i)$ such that the cardinality of $Z := \{w \in B : (z, w) \in \pi_i(T_i)\}$ is at least K'. Fix such z. Then $Z \in \mathcal{B}(\Pi^{(1)}_{y,z})$. As T_i only contains i-small blocks, every block in $\Pi^{(1)}_{y,z}$ contained in Z has cardinality at most K'. By removing some of these blocks if necessary, we obtain a subset $Z' \subseteq Z$ such that $Z' \in \mathcal{B}(\Pi^{(1)}_{y,z})$ and $K' \leq |Z'| \leq 2K' = O(|B|/K')$.

Choose $B' = Z'$. Note $(y, z) \in B^{k'}$ where $k' := kr + i - 1$. To see Lemma 17 is satisfied by B', it suffices to show $K' = 2^{\Omega(k'(\rho^2 \log\log\log\log n)^{1/3})}$. This holds since $k' = O(r/\rho(B))$, $K' = (\log\log\log n)^{r\rho(B)}$, and $\rho(B) \geq (\rho/\log\log\log\log n)^{1/3}$.

Case 2: $|T_i| < K'|B|^{k-1}$ **for all** $i \in [k]$**.** So $\sum_{i=1}^k |T_i| < kK'|B|^{k-1} = |B|^{k-1}2^{(\log n)^{o(1)}}$. As $\sigma_k|_A : A \to A'$ is bijective, we also have

$$|A'| = |A| \geq |B|^k/K^{(k-1)/2} = |B|^k/2^{(\log n)^{o(1)}}.$$

Using the facts $|B| \geq n^{1/(\rho^2 \log\log\log\log n)^{1/3}}$ and $|T| = |A''| \geq |A'|/2^{(\log n)^{1/2}}$, we see $|T| > \sum_{i=1}^k |T_i|$. Therefore, there exists a block $U \in \Pi^{(k)}_y$ such that $U \subseteq T$ and U is not i-small for $i \in [k]$. Note $|U| = \prod_{i=1}^k |\pi_i(U)|/|\pi_{i-1}(U)|$. Fix $i \in [k]$ that minimizes $|\pi_i(U)|/|\pi_{i-1}(U)|$. Then

$$|\pi_i(U)|/|\pi_{i-1}(U)| \leq |U|^{1/k} \leq |T|^{1/k} = |A''|^{1/k} \leq \left(|A|/2^{-Cr\log\log\log\log n}\right)^{1/k} \leq |B|/K'^{\Omega(1)}.$$

As U is not i-small, we also have $|\pi_i(U)|/|\pi_{i-1}(U)| \geq K'$. Pick $z \in \pi_{i-1}(U)$. Let $B' = \{w \in B : (z, w) \in \pi_i(T_i)\}$. Then $B' \in \mathcal{B}(\Pi^{(1)}_{y,z})$, $|B'| = |\pi_i(U)|/|\pi_{i-1}(U)|$, and $(y, z) \in B^{k'}$, where $k' = kr + i - 1$. As in the previous case, we have $K' = 2^{\Omega(k'(\rho^2 \log\log\log\log n)^{1/3})}$. So Lemma 17 is satisfied by B'. ◀

5 Conclusion

It is natural to ask how to simplify our proof and/or improve our bounds. The bottleneck is Lemma 21, whose proof suffer exponential loss in several places, resulting in the weak $(\rho^2 \log\log\log\log n)^{1/3}$ improvement. One place is the Freiman–Ruzsa Theorem (Theorem 6), where the bound $|\langle A\rangle|/|A| \leq \ell^{2K}$ is exponential in K. One natural idea is replacing it by the quasi-polynomial Freiman-Ruzsa Theorem [33]. However, it is not clear to us if the latter can be made constructive enough to be compatible with our notion of linear m-schemes. Another place is Theorem 32, which gives the bound $h(A) = O(1/\mu(A))$. We suspect it may be improved to $h(A) = \tilde{O}(\log(1/\mu(A)))$ when the ambient space V is defined over a small prime field $\mathbb{F}$. Indeed, this was achieved in [25] for the special case $\mathbb{F} = \mathbb{F}_2$.

References

1 L. Adleman, K. Manders, and G. Miller. On taking roots in finite fields. In *Proceedings of the 18th Annual Symposium on Foundations of Computer Science*, pages 175–178, 1977.

2 M. Arora. *Extensibility of association schemes and GRH-based deterministic polynomial factoring.* PhD thesis, Universitäts-und Landesbibliothek Bonn, 2013.

3 M. Arora, G. Ivanyos, M. Karpinski, and N. Saxena. Deterministic polynomial factoring and association schemes. *LMS Journal of Computation and Mathematics*, 17(01):123–140, 2014.

4 A. Balog and E. Szemerédi. A statistical theorem of set addition. *Combinatorica*, 14(3):263–268, 1994.

5 E. R. Berlekamp. Factoring polynomials over finite fields. *Bell System Technical Journal*, 46(8):1853–1859, 1967.

6 E. R. Berlekamp. Factoring polynomials over large finite fields. *Mathematics of Computation*, 24(111):713–735, 1970.

7 J. Bourgain, S. Konyagin, and I. Shparlinski. Character sums and deterministic polynomial root finding in finite fields. *Mathematics of Computation*, 84(296):2969–2977, 2015.

8 Q. Cheng and M. A. Huang. Factoring polynomials over finite fields and stable colorings of tournaments. In *Proceedings of the 4th Algorithmic Number Theory Symposium*, pages 233–245, 2000.

9 S. A. Evdokimov. Factorization of solvable polynomials over finite fields and the generalized Riemann hypothesis. *Journal of Soviet Mathematics*, 59(3):842–849, 1992.

10 S. A. Evdokimov. Factorization of polynomials over finite fields in subexponential time under GRH. In *Proceedings of the 1st Algorithmic Number Theory Symposium*, pages 209–219, 1994.

11 C. Even-Zohar. On sums of generating sets in $\mathbb{Z}_2^n$. *Combinatorics, probability and computing*, 21(6):916–941, 2012.

12 C. Even-Zohar and S. Lovett. The Freiman–Ruzsa theorem over finite fields. *Journal of Combinatorial Theory, Series A*, 125:333–341, 2014.

13 S. Gao. On the deterministic complexity of factoring polynomials. *Journal of Symbolic Computation*, 31(1):19–36, 2001.

14 W. T. Gowers. A new proof of Szemerédi's theorem for arithmetic progressions of length four. *Geometric and Functional Analysis*, 8(3):529–551, 1998.

15 Y. Guan. *Factoring polynomials and Gröbner bases*. PhD thesis, Clemson University, 2009.

16 Z. Guo. *$\mathcal{P}$-schemes and deterministic polynomial factoring over finite fields*. PhD thesis, Caltech, 2017.

17 Z. Guo. Deterministic polynomial factoring over finite fields with restricted Galois groups, 2019. Manuscript. `https://zeyuguo.bitbucket.io/papers/galois.pdf`.

18 Z. Guo. Deterministic polynomial factoring over finite fields: a uniform approach via $\mathcal{P}$-schemes. *Journal of Symbolic Computation*, 96:22 – 61, 2020.

19 Y. O. Hamidoune and Ø. Rødseth. On bases for σ-finite groups. *Mathematica Scandinavica*, pages 246–254, 1996.

20 M. A. Huang. Factorization of polynomials over finite fields and decomposition of primes in algebraic number fields. *Journal of Algorithms*, 12(3):482 – 489, 1991.

21 M. A. Huang. Generalized Riemann hypothesis and factoring polynomials over finite fields. *Journal of Algorithms*, 12(3):464 – 481, 1991.

22 G. Ivanyos, M. Karpinski, L. Rónyai, and N. Saxena. Trading GRH for algebra: algorithms for factoring polynomials and related structures. *Mathematics of Computation*, 81(277):493–531, 2012.

23 G. Ivanyos, M. Karpinski, and N. Saxena. Schemes for deterministic polynomial factoring. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, pages 191–198, 2009.

24 B. Klopsch and V. F. Lev. How long does it take to generate a group? *Journal of Algebra*, 261(1):145–171, 2003.

25 V. F. Lev. Generating binary spaces. *Journal of Combinatorial Theory, Series A*, 102(1):94–109, 2003.

26 G. Malle and B. H. Matzat. *Inverse Galois Theory*. Springer, 1999.

27 J. Neukirch. *Algebraic Number Theory*. Springer-Verlag, 1999.

28 J. Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Mathematics of Computation*, 55(192):745–763, 1990.

29 L. Rónyai. Factoring polynomials over finite fields. *Journal of Algorithms*, 9(3):391–400, 1988.

30 L. Rónyai. Factoring polynomials modulo special primes. *Combinatorica*, 9(2):199–206, 1989.

31 L. Rónyai. Galois groups and factoring polynomials over finite fields. *SIAM Journal on Discrete Mathematics*, 5(3):345–365, 1992.

32 I. Z. Ruzsa. An analog of Freiman's theorem in groups. *Asterisque*, 258:323–326, 1999.

33 T. Sanders. On the Bogolyubov–Ruzsa lemma. *Analysis & PDE*, 5(3):627–655, 2012.

34 R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, 44(170):483–494, 1985.

35 V. Shoup. On the deterministic complexity of factoring polynomials over finite fields. *Information Processing Letters*, 33(5):261–267, 1990.

36 V. Shoup. Smoothness and factoring polynomials over finite fields. *Information Processing Letters*, 38(1):39–42, 1991.

37 T. Tao and V. H. Vu. *Additive Combinatorics*, volume 105. Cambridge University Press, 2006.

38 J. von zur Gathen. Factoring polynomials and primitive elements for special primes. *Theoretical Computer Science*, 52(1):77–89, 1987.

39 D. Y.Y. Yun. On square-free decomposition algorithms. In *Proceedings of the 3rd ACM Symposium on Symbolic and Algebraic Computation*, pages 26–35, 1976.

A $\mathcal{P}$-schemes

Notations. A *(left) action* of a group G on a set S is a function $\varphi : G \times S \to S$ satisfying (1) $\varphi(e, x) = x$ for all $x \in S$ and (2) $\varphi(g, \varphi(h, x)) = \varphi(gh, x)$ for $x \in S$ and $g, h \in G$. We also write ${}^g x$ for $\varphi(g, x)$. The *orbit* or *G-orbit* of $x \in S$ is $Gx := \{{}^g x : g \in G\}$. The *stabilizer* of $x \in S$ is $G_x := \{g \in G : {}^g x = x\}$. For $T \subseteq S$, the *pointwise stabilizer* of T is $G_T := \{g \in G : {}^g x = x \text{ for } x \in T\}$. When $T = \{x_1, \ldots, x_k\}$, we also write $G_{x_1,\ldots,x_k}$ for G_T.

$\mathcal{P}$-schemes. We recall the definition of $\mathcal{P}$-schemes in [18]: Let G be a finite group. A set $\mathcal{P}$ of subgroups of G is called a *subgroup system over G* if $\mathcal{P}$ is closed under conjugation, i.e., $gHg^{-1} \in \mathcal{P}$ for $H \in \mathcal{P}$ and $g \in G$. Define the following two kinds of maps between right coset spaces $H\backslash G$ for various subgroups $H \leq G$:

- For $H \leq H' \leq G$, define the *projection* $\pi_{H,H'} : H\backslash G \to H'\backslash G$ to be the map sending $Hg \in H\backslash G$ to $H'g \in H'\backslash G$.
- For $H \leq G$ and $g \in G$, define the *conjugation* $c_{H,g} : H\backslash G \to gHg^{-1}\backslash G$ to be the map sending $Hh \in H\backslash G$ to $(gHg^{-1})gh \in gHg^{-1}\backslash G$.

▶ **Definition 26** ($\mathcal{P}$-scheme [18]). *Let $\mathcal{P}$ be a subgroup system over G. A* $\mathcal{P}$-collection *is a set $\mathcal{C} = \{C_H : H \in \mathcal{P}\}$ indexed by $\mathcal{P}$, where C_H is a partition of $H\backslash G$ for $H \in \mathcal{P}$. Moreover, we say $\mathcal{C}$ is a* $\mathcal{P}$-scheme *if it has the following properties:*

(Compatibility): *For $H, H' \in \mathcal{P}$ with $H \leq H'$ and $x, x' \in H\backslash G$ in the same block of C_H, $\pi_{H,H'}(x)$ and $\pi_{H,H'}(x')$ are in the same block of $C_{H'}$.*

(Invariance): *For $H \in \mathcal{P}$ and $g \in G$, the map $c_{H,g} : H\backslash G \to gHg^{-1}\backslash G$ maps any block of C_H bijectively to a block of $C_{gHg^{-1}}$.*

(Regularity): *For $H, H' \in \mathcal{P}$ with $H \leq H'$, any block $B \in C_H$, $B' \in C_{H'}$, the number of $x \in B$ satisfying $\pi_{H,H'}(x) = y$ is constant when y ranges over the set B'.*

In addition, $\mathcal{C}$ is discrete *on $H \in \mathcal{P}$ if C_H is the finest partition of $H\backslash G$. It is* strongly antisymmetric *if no nontrivial permutation of any block in any partition C_H can be obtained by composing maps of the form $c_{H_{i-1},g}|_{B_{i-1}}$, $\pi_{H_{i-1},H_i}|_{B_{i-1}}$, or $(\pi_{H_i,H_{i-1}}|_{B_i})^{-1}$.*

Now suppose G is a permutation group on a finite set S. For $m \in \mathbb{N}^+$, define $\mathcal{P}_m := \{G_{x_1,\ldots,x_k} : k \in [m],\ x_1, \ldots, x_k \in S\}$, which is a subgroup system over G, called the *system of stabilizers of depth m*. Denote by $d(G)$ the smallest $m \in \mathbb{N}^+$ such that every strongly antisymmetric $\mathcal{P}_m$-scheme is discrete on G_x for all $x \in S$. Then $d(G)$ is well defined and we have

▶ **Theorem 27** ([18, Theorem 1.3]). *Under GRH, there exists a deterministic algorithm that, given $f(X) \in \mathbb{F}_p[X]$ of degree n that factorizes into n distinct linear factors over $\mathbb{F}_p$ and a*

lifted polynomial $\tilde{f}(X) \in \mathbb{Z}[X]$ with the Galois group G acting on the set of roots of $\tilde{f}(X)$, completely factorizes $f(X)$ over $\mathbb{F}_p$ in time polynomial in $n^{d(G)}$ and the size of the input.

From a $\mathcal{P}_m$-scheme to a linear m-scheme. Now suppose $G \leq \mathrm{GL}(V)$ acts linearly on $S \subseteq V$, where V is a vector space over a finite field $\mathbb{F}$. Let $m \in \mathbb{N}^+$, and let $\mathcal{C} = \{C_H : H \in \mathcal{P}_m\}$ be a $\mathcal{P}_m$-scheme. We will use $\mathcal{C}$ to construct a linear m-scheme $\Pi(\mathcal{C})$ on S.

For $k \in [m]$, equip S^k with the diagonal action of G. Then $\mathcal{P}_m = \{G_x : x \in S^k, k \in [m]\}$. For a subgroup $H \leq G$, equip $H\backslash G$ with the *inverse right action* of G, i.e., ${}^g Hh = Hhg^{-1}$ for $Hh \in H\backslash G$ and $g \in G$. For $k \in [m]$ and $x \in S^k$, let λ_x be the map $Gx \to G_x\backslash G$ sending ${}^g x \in Gx$ to $G_x g^{-1}$ for $g \in G$. Then λ_x is a well defined bijection and is G-*equivariant*, i.e., $\lambda_x({}^g \cdot) = {}^g \lambda_x(\cdot)$ for $g \in G$.

▶ **Definition 28.** *For a $\mathcal{P}_m$-scheme $\mathcal{C} = \{C_H : H \in \mathcal{P}_m\}$, let*

$$\Pi(\mathcal{C}) := \{\Pi(\mathcal{C})^{(1)}, \ldots, \Pi(\mathcal{C})^{(m)}\}$$

where for $k \in [m]$, $\Pi(\mathcal{C})^{(k)}$ is a partition of S^k defined as follows: elements of S^k are in different blocks of $\Pi(\mathcal{C})^{(k)}$ if they are in different G-orbits. For each G-orbit O, choose $x \in O$ so that $O = Gx$ and we have a bijection $\lambda_x : O \to G_x\backslash G$. Then define the partition $\Pi(\mathcal{C})^{(k)}|_O$ of O to be $\lambda_x^{-1}(C_{G_x})$.

▶ **Lemma 29.** *$\Pi(\mathcal{C})$ is well defined linear m-scheme on S independent of the choices of the elements x. Moreover, if $\mathcal{C}$ is strongly antisymmetric, so is $\Pi(\mathcal{C})$.*

Proof. For $x' = {}^g x$, $g \in G$, we have $\lambda_{x'} = c_{G_x, g} \circ \lambda_x$. It follows from invariance of $\mathcal{C}$ that $\Pi(\mathcal{C})^{(k)}|_O$ does not depend on the choice of $x \in O$. So $\Pi(\mathcal{C})$ is well defined.

Next we prove that $\Pi(\mathcal{C})$ is a linear m-scheme on S. Let $\tau \in \mathcal{M}_{k,k'}$ where $k, k' \in [m]$. Then τ has the form

$$\mathbf{x} = (x_1, \ldots, x_k) \mapsto \left(\sum_{i=1}^{k} c_{i,1} x_i, \ldots, \sum_{i=1}^{k} c_{i,k'} x_i \right), \quad \text{where } c_{i,j} \in \mathbb{F}.$$

As $G \leq \mathrm{GL}(V)$ acts linearly on S, and diagonally on S^k and $S^{k'}$, we have

$${}^g \tau(\mathbf{x}) = {}^g \left(\sum_{i=1}^{k} c_{i,1} x_i, \ldots, \sum_{i=1}^{k} c_{i,k'} x_i \right) = \left(\sum_{i=1}^{k} c_{i,1} {}^g x_i, \ldots, \sum_{i=1}^{k} c_{i,k'} {}^g x_i \right) = \tau({}^g \mathbf{x}),$$

i.e., τ is G-equivariant. Then for $x \in S^k$ such that $\tau(x) \in S^{k'}$, we have $G_x \leq G_{\tau(x)}$ and the following diagram commutes.

$$\begin{array}{ccc} Gx & \xrightarrow{\tau|_{Gx}} & G\tau(x) \\ {\scriptstyle \lambda_x}\downarrow & & \downarrow{\scriptstyle \lambda_{\tau(x)}} \\ G_x\backslash G & \xrightarrow{\pi_{G_x, G_{\tau(x)}}} & G_{\tau(x)}\backslash G\,. \end{array} \tag{3}$$

Also note that the maps λ_x and $\lambda_{\tau(x)}$ are bijections, sending blocks to blocks. The properties (P1) and (P2) of $\Pi(\mathcal{C})$ then follow from compatibility and regularity of $\mathcal{C}$. So $\Pi(\mathcal{C})$ is a linear m-scheme.

Now assume $\Pi(\mathcal{C})$ is not strongly antisymmetric and we prove $\mathcal{C}$ is not either. By definition, for some $k \in [m]$, there exists a nontrivial permutation $\tau \in \widetilde{\mathcal{M}}_{\Pi(\mathcal{C})}$ of a block $B \in \Pi(\mathcal{C})^{(k)}$. Using Diagram (3), we see that there exist $x, x' \in B$, and a map $\widetilde{\tau} : \widetilde{B} \to \widetilde{B'}$

that is a composition of maps of the form $\pi_{H,H'}|_{B'}$ or $(\pi_{H,H'}|_{B'})^{-1}$ (where $H, H' \in \mathcal{P}_m$ and B' is a block) such that the following diagram commutes.

$$\begin{array}{ccc} B & \xrightarrow{\tau} & B \\ {\scriptstyle\lambda_x}\downarrow & & \downarrow{\scriptstyle\lambda_{x'}} \\ \widetilde{B} & \xrightarrow{\widetilde{\tau}} & \widetilde{B}'. \end{array}$$

By construction, B is a subset of a G-orbit of S^k. So $x' = {}^g x$ for some $g \in G$. Note $\lambda_{x'} = c_{G_x,g} \circ \lambda_x$. By replacing $\widetilde{\tau}$ with $\widetilde{\tau} \circ c^{-1}_{G_x,g}$, x with x', and $\widetilde{B}$ with $\widetilde{B}'$ respectively, we may assume $x = x'$ and $\widetilde{B} = \widetilde{B}'$. Then as τ is a nontrivial permutation, so is $\widetilde{\tau}$. So $\mathcal{C}$ is not strongly antisymmetric. ◀

Now we are ready to derive Theorem 1 from Theorem 5 (together with the more elementary Lemma 16).

Proof of Theorem 1 . Let $G = \mathrm{GL}(V)$ act linearly on $S \subseteq V$. We will prove $d(G) = O(\log n)$, $d(G) \leq \dim\langle S\rangle_{\mathbb{F}}$, and $d(G) = O\left(\frac{\log n}{(\rho^2 \log\log\log\log n)^{1/3}}\right)$. Theorem 1 then follows directly from Theorem 27.

If $d(G) = 1$ then we are done. So assume $d(G) > 1$. Let $m = d(G) - 1 < d(G)$. Then there exists a strongly antisymmetric $\mathcal{P}_m$-scheme $\mathcal{C}$ on S that is not discrete on G_x for some $x \in S$. By Lemma 29, $\Pi(\mathcal{C})$ is a strongly antisymmetric linear m-scheme on S. As $\mathcal{C}$ is not discrete on G_x, $\Pi(\mathcal{C})^{(1)}$ is not the finest partition of S. We then have $m \leq \log n$ and $m < \dim\langle S\rangle_{\mathbb{F}}$ by Lemma 16. Then $d(G) = m + 1$ satisfies $d(G) = O(\log n)$ and $d(G) \leq \dim\langle S\rangle_{\mathbb{F}}$. Similarly, $d(G) = m + 1 = O\left(\frac{\log n}{(\rho^2 \log\log\log\log n)^{1/3}}\right)$ holds by Theorem 5. ◀

Next, we define the function $d_{\mathrm{Lin}}(m, q)$ and prove Theorem 3.

▶ **Definition 30** ([17]). *For $m \in \mathbb{N}^+$ and a prime power q, define $d_{\mathrm{Lin}}(m, q)$ to be the maximum possible value of $d(G)$, where $G \leq \mathrm{GL}_{m'}(q')$ acts linearly on a set $S \subseteq \mathbb{F}_{q'}^{m'}$, and (m', q') ranges over the set of pairs satisfying $m' \leq m$, $q'^{m'} \leq q^m$ and $\gcd(q, q') \neq 1$.*

Proof of Theorem 3. Let $m \in \mathbb{N}^+$ and q be a prime power. Let G act linearly on a subset $S \subseteq \mathbb{F}_{q'}^{m'}$ where $m' \leq m$, $q'^{m'} \leq q^m$ and $\gcd(q, q') \neq 1$. Suppose $m_0 \in \mathbb{N}^+$ and $\mathcal{C}$ is a strongly antisymmetric $\mathcal{P}_{m_0}$-scheme on S that is not discrete on G_x for some $x \in S$. We want to prove $m_0 = O\left(\frac{m \log q}{(\log\log\log(m \log q))^{1/3}}\right)$.

By Lemma 29, $\Pi(\mathcal{C})$ is a strongly antisymmetric linear m_0-scheme on S. As $\mathcal{C}$ is not discrete on G_x, $\Pi(\mathcal{C})^{(1)}$ is not the finest partition of S. By Theorem 5, we have $m_0 = O\left(\frac{\log n}{(\rho^2 \log\log\log\log n)^{1/3}}\right)$ where $\rho = \log|S|/\log|\langle S\rangle|$ and $n = |S| = |\langle S\rangle|^\rho \leq q^{\rho m}$. Combining this bound with the facts $\rho \leq 1$ and $\log n \leq \rho m \log q$ gives the desired bound. ◀

Finally, we prove Corollary 4.

Proof of Corollary 4. By the definition of $N_{\mathcal{C}}(G)$ [17, Theorem 1.2], we have $N_{\mathcal{C}}(G) = q_0^{m_0 d_{\mathrm{Lin}}(cm_0, q_0)}$, where G has a nonabelian composition factor that is a classical group of rank m_0 over $\mathbb{F}_{q_0}$ and $c \in \mathbb{N}^+$ is an absolute constant. Here $q_0^{m_0} = n^{O(1)}$ by [17, Corollary 4.10]. So $d_{\mathrm{Lin}}(cm_0, q_0) = O\left(\frac{n}{(\log\log\log\log n)^{1/3}}\right) = o(\log n)$ by Theorem 3. It follows that $N_{\mathcal{C}}(G) = n^{o(\log n)}$.

To prove the second statement, it suffices to prove $N_{\mathcal{A}}(G) = n^{o(\log n)}$. By the definition of $N_{\mathcal{A}}(G)$ [17, Theorem 1.2], we have $N_{\mathcal{A}}(G) = m_1^{d_{\mathrm{Sym}}(m_1^c)}$, where G has a nonabelian

composition factor that is an alternating group of degree m_1 and $c \in \mathbb{N}^+$ is an absolute constant. By assumption, we have $m_1 = n^{o(1)}$. Now $N_{\mathcal{A}}(G) = n^{o(\log n)}$ follows from $d_{\mathrm{Sym}}(m) = O(\log m)$ [17, Lemma 3.18]. ◀

B Omitted Proofs in Section 3

Proof of Lemma 10. Assume $\sum_{i=1}^{k} c_i x_i = 0$ and we prove that $\sum_{i=1}^{k} c_i y_i = 0$. The claim is trivial if all c_i are zero. By symmetry, we may assume $c_k \neq 0$. By scaling, we may further assume $c_k = -1$, i.e., $x_k = \sum_{i=1}^{k-1} c_i x_i$. Let $\tau \in \mathcal{M}_{k,k}$ be the map $(a_1, \ldots, a_{k-1}, a_k) \mapsto (a_1, \ldots, a_{k-1}, \sum_{i=1}^{k-1} c_i a_i)$. We have $\mathbf{x} = \tau(\mathbf{x}) \in \tau(B)$. Then $\tau(B) = B$ by Property (P1). So $\mathbf{y} \in \tau(B)$. But $\sum_{i=1}^{k} c_i a_i = 0$ holds for all $(a_1, \ldots, a_k) \in \tau(B)$. So $\sum_{i=1}^{k} c_i y_i = 0$. ◀

Proof of Lemma 12. Claim (1) holds since $\Pi^{(k)}$ is a partition of S^k. To prove (2), first consider the case $Q = \exists_{=t}$ where $t \in \mathbb{N}$. Suppose B is the disjoint union of $B_1, \ldots, B_s \in \Pi^{(k+k')}$. Then

$$B_{\exists_{=t}} = \bigcup_{\substack{t_1,\ldots,t_s \in \mathbb{N} \\ t_1+\cdots+t_s=t}} \bigcap_{i=1}^{s} (B_i)_{\exists_{=t_i}}.$$

So we may assume $B \in \Pi^{(k+k')}$. Let $\pi \in \mathcal{M}_{k+k',k}$ be the projection sending $(x, y) \in V^k \times V^{k'}$ to $x \in V^k$. Let $B' \in \Pi^{(k)}$. For $x \in B'$, we have $x \in B_{\exists_{=t}}$ iff $\#\{y \in S^{k'} : (x, y) \in B\} = t$. We also know that $\#\{y \in S^{k'} : (x, y) \in B\} = \#\{z \in B : \pi(z) = x\}$ is constant when x ranges over B'. So either $B' \subseteq B_{\exists_{=t}}$ or $B' \cap B_{\exists_{=t}} = \emptyset$. Therefore $B_{\exists_{=t}}$ is a disjoint union of blocks in $\Pi^{(k)}$, i.e., $B_{\exists_{=t}} \in \mathcal{B}(\Pi^{(k)})$. This proves (2) for the case $Q = \exists_{=t}$. The case $Q = \exists$ follows since $B_{\exists} = \bigcup_{t \in \mathbb{N}^+} B_{\exists_{=t}}$. The case $Q = \forall$ also follows since $B_{\forall}$ is the complement of $\overline{B}_{\exists}$ in S^k, where $\overline{B}$ denotes the complement of B in $S^{k+k'}$.

To prove (3), suppose B is the disjoint union of $B_1, \ldots, B_s \in \Pi^{(k)}$. Then $\tau(B) \cap S^{k'} = \bigcup_{i=1}^{s} (\tau(B_i) \cap S^{k'})$. So we may assume $B \in \Pi^{(k)}$. If $\tau(B) \cap S^{k'} = \emptyset$, then trivially $\tau(B) \cap S^{k'} \in \mathcal{B}(\Pi^{(k')})$. So assume $\tau(B) \cap S^{k'} \neq \emptyset$. Choose $B' \in \Pi^{(k')}$ such that $\tau(B) \cap B' \neq \emptyset$. Then $\tau(B) = B' \in \mathcal{B}(\Pi^{(k')})$ by Property (P1) of linear m-schemes.

To prove (4), suppose B is the disjoint union of $B_1, \ldots, B_s \in \Pi^{(k')}$. Then $\tau^{-1}(B) \cap S^k = \bigcup_{i=1}^{s} (\tau^{-1}(B_i) \cap S^k)$. So we may assume $B \in \Pi^{(k')}$. By Property (P1), for every $B' \in \Pi^{(k)}$ intersecting $\tau^{-1}(B) \cap S^k$ (i.e. $\tau(B') \cap B \neq \emptyset$), we have $\tau(B') = B$, which implies $B' \subseteq \tau^{-1}(B) \cap S^k$. So $\tau^{-1}(B) \cap S^k$ is a disjoint union of blocks in $\Pi^{(k)}$, i.e., $\tau^{-1}(B) \cap S^k \in \mathcal{B}(\Pi^{(k)})$. ◀

Proof of Lemma 14. As $\Pi_{x_1,\ldots,x_t} = (\Pi_{x_1,\ldots,x_{t-1}})_{x_t}$, it suffices to prove the claim for $t = 1$. So assume $t = 1$ and $x = x_1$. For $k \in [m-1]$ and $B \in \Pi_x^{(k)}$, let $\widetilde{B}$ be the block in $\Pi^{(k+1)}$ satisfying $B = \{y \in S^k : (x, y) \in \widetilde{B}\}$. For $k, k' \in [m-1]$ and $\tau \in \mathcal{M}_{k,k'}$, denote by $\widetilde{\tau} : V^{k+1} \to V^{k'+1}$ the map sending $(u, v) \in V \times V^k$ to $(u, \tau(v))$, which is in $\mathcal{M}_{k+1,k'+1}$.

For $k \in [m-1]$, identify V^k with $\pi_{k+1,1}^{-1}(x) \subseteq V^{k+1}$ via $y \mapsto (x, y)$. Then S^k is identified with the set $S^{k+1} \cap \pi_{k+1,1}^{-1}(x)$. Then $\Pi_x^{(k)}$ becomes a partition of $S^{k+1} \cap \pi_{k+1,1}^{-1}(x)$, which is precisely $\Pi^{(k+1)}|_{S^{k+1} \cap \pi_{k+1,1}^{-1}(x)}$. A block $B \in \Pi_x^{(k)}$ is then identified with $\widetilde{B} \cap \pi_{k+1,1}^{-1}(x)$. For $k, k' \in [m-1]$, a map $\tau \in \mathcal{M}_{k,k'}$ is identified with

$$\widetilde{\tau}|_{\pi_{k+1,1}^{-1}(x)} : \pi_{k+1,1}^{-1}(x) \to \pi_{k'+1,1}^{-1}(x).$$

Consider $k, k' \in [m-1]$, $B \in \Pi^{(k+1)}$, $B' \in \Pi^{(k'+1)}$, and $\tau \in \mathcal{M}_{k,k'}$. As Π is a linear m-scheme, we have

1. $\widetilde{\tau}(B)$ and B' are either the same or disjoint from each other, and
2. $\#\{z \in B : \widetilde{\tau}(z) = y\}$ is constant when y ranges over B'.

As $\widetilde{\tau}$ fixes the first coordinate, it sends $\pi_{k+1,1}^{-1}(t)$ to $\pi_{k'+1,1}^{-1}(t)$ for $t \in V$. Therefore

1. $\widetilde{\tau}(B \cap \pi_{k+1,1}^{-1}(x))$ and $B' \cap \pi_{k'+1,1}^{-1}(x)$ are either the same or disjoint from each other, and
2. for $y \in B' \cap \pi_{k'+1,1}^{-1}(x)$, $\#\{z \in B \cap \pi_{k+1,1}^{-1}(x) : \widetilde{\tau}(z) = y\} = \#\{z \in B : \widetilde{\tau}(z) = y\}$, which is constant when y ranges over $B' \cap \pi_{k'+1,1}^{-1}(x)$.

This shows that Π_x is a linear m-scheme by the above identifications.

Assume Π_x is not strongly antisymmetric. Then there exists a sequence of bijections $\tau_i : B_{i-1} \to B_i$, $i = 1, \dots, s$, whose composition is a nontrivial permutation of $B_0 = B_s$, and for $i \in [s]$, either τ_i or τ_i^{-1} is in $\mathcal{M}_{\Pi_x}$. Suppose $B_i \in \Pi_x^{(k_i)}$ for $i = 0, \dots, s$, where $k_i \in [m-1]$. We have identified B_i with $\widetilde{B}_i \cap \pi_{k_i}^{-1}(x)$ for unique $\widetilde{B}_i \in \Pi^{(k_i+1)}$. Each map τ_i then extends to a bijection $\widetilde{\tau}_i : \widetilde{B}_{i-1} \to \widetilde{B}_i$ such that either $\widetilde{\tau}_i$ or $\widetilde{\tau}_i^{-1}$ is in $\mathcal{M}_\Pi$. The composition of these maps $\widetilde{\tau}_i$ or their inverses then gives a nontrivial permutation of $\widetilde{B}_0 = \widetilde{B}_s$. So Π is not strongly antisymmetric. ◀

Proof of Lemma 16. (1): Let $k = \dim\langle S\rangle_{\mathbb{F}}$. Assume to the contrary that $m \geq k$. Let T be the set of $(x_1, \dots, x_k) \in S^k$ such that the coordinates x_i are linearly independent over $\mathbb{F}$. By Lemma 10, we have $T \in \mathcal{B}(\Pi^{(k)})$.

Assume $\mathbf{x} = (x_1, \dots, x_k), \mathbf{y} = (x_1, \dots, x_k) \in T$ are in the same block $B \in \Pi^{(k)}$. As the coordinates of $\mathbf{x}$ as well as those of $\mathbf{y}$ form a basis of $\langle S\rangle_{\mathbb{F}}$, there exists an invertible linear map $\tau \in \mathcal{M}_{k,k}$ sending $\mathbf{x}$ to $\mathbf{y}$. So $\mathbf{y} \in \tau(B) \cap B$. Then $\tau(B) = B$ by Property (P1). As Π is strongly antisymmetric, we must have $\mathbf{x} = \mathbf{y}$. This shows that T is a disjoint union of singletons in $\Pi^{(k)}$, i.e., $\Pi^{(k)}|_T = \infty_T$. Also note $\pi_{k,1} \in \mathcal{M}_{k,1}$ maps T surjectively to S. It follows from Lemma 12 (3) that $\Pi^{(1)} = \infty_S$, contradicting the assumption that B is not a singleton. So $m < k = \dim\langle S\rangle_{\mathbb{F}}$.

(2): The proof here is the same as the proof for m-schemes in [23], which essentially goes back to [10]. We first prove the following claim.

▷ Claim 31. Suppose Π is a strongly antisymmetric linear m-scheme on $S \subseteq V$, where $m \geq 2$, and $B \in \Pi^{(1)}$ is not a singleton. Let x, y be distinct elements in B. Let B' be the block in $\Pi_x^{(1)}$ containing y. Then $1 < |B'| \leq |B|/2$.

Proof. Let $\tau : V^2 \to V^2$ be the permutation $(a, b) \mapsto (b, a)$. Then $\tau \in \mathcal{M}_{2,2}$. Let B'' be the block in $\Pi^{(2)}$ containing (x, y). Note $\tau(B'') \in \Pi^{(2)}$ by Property (P1). As $x, y \in B$, the projections $\pi_{2,1}$ and $\pi_{2,2}$ both map B'' and $\tau(B'')$ surjectively to B by Property (P1). So $B'', \tau(B'') \subseteq B \times B$. As $\tau(x, y) = (y, x) \neq (x, y)$, we have $\tau(B'') \neq B''$ by strong antisymmetry of Π. So $|B''| = |\tau(B'')| \leq |B|^2/2$. Then by Property (P2), we have $|B'| = |B''|/|B| \leq |B|/2$. Finally, assume to the contrary $|B'| = 1$. Then $\pi_{2,1}|_{B''} : B'' \to B$ and $\pi_{2,2}|_{B''} : B'' \to B$ are bijective by Property (P2). The map $\pi_{2,2}|_{B_1} \circ (\pi_{2,1}|_{B_1})^{-1}$ sends x to y, and hence is a nontrivial permutation of B. But this contradicts strong antisymmetry of Π. So $|B'| > 1$. ◀

Lemma 16 (2) now follows from Claim 31, Lemma 14, and induction on m. ◀

C Omitted Proofs in Section 4

This section contains the proofs omitted in Section 4 except that of Lemma 21. We prove Lemma 21 in Appendix D.

Proof of Lemma 18. Let $k \in [m-2]$, $x_1, \dots, x_k \in B$, $B' \in \mathcal{B}(\Pi_{x_1,\dots,x_k}^{(1)})$, and $C > 0$ be as in Lemma 17. In addition, let $t := (\rho^2 \log\log\log\log n)^{1/3}$. As $\min\{|B'|, |B|/|B'|\} \geq 2^{Ckt}$,

we have $|B| \geq 2^{2Ckt}$. We will find $k' \in [k]$, $y_1, \ldots, y_{k'} \in B$, and $B'' \in \Pi^{(1)}_{y_1,\ldots,y_{k'}}$ such that $B'' \subseteq B$, $|B''| > 1$ and $|B|/|B''| = 2^{\Omega(kt)} = 2^{\Omega(k(\rho^2 \log\log\log\log n)^{1/3})}$. The condition $B'' \neq B$ follows automatically from $|B''| > 1$: By Lemma 10, we have $\{y_1\} \in \Pi^{(1)}_{y_1,\ldots,y_{k'}}$ and hence $y_1 \notin B''$. So $B'' \neq B$.

If $\Pi^{(1)}_{x_1,\ldots,x_k}|_{B'} \neq \infty_{B'}$, we can find $B'' \in \Pi^{(1)}_{x_1,\ldots,x_k}$ contained in B' satisfying $|B''| > 1$. In this case, let $k' = k$ and $y_i = x_i$ for $i \in [k]$, and we are done. So assume $\Pi^{(1)}_{x_1,\ldots,x_k}|_{B'} = \infty_{B'}$.

For $0 \leq i \leq k$, let T_i be the set of $x \in B'$ satisfying $\{x\} \in \Pi^{(1)}_{x_1,\ldots,x_i}$. We have $T_0 = \emptyset$, $T_k = B'$, and $T_{i-1} \subseteq T_i$ for $i \in [k]$ by Lemma 15. So there exists $i \in [k]$ such that $|T_i \setminus T_{i-1}| \geq |B'|/k \geq 2^{Ckt}/k = 2^{\Omega(kt)}$. Fix such i and let $\Pi' = \Pi_{x_1,\ldots,x_{i-1}}$. By Lemma 14, Π' is a strongly antisymmetric linear $(m-i+1)$-scheme, where $m - i + 1 \geq m - k + 1 \geq 3$.

First assume $i = 1$. By Claim 31 in the proof of Lemma 16, $\{x_1\}$ is the only singleton in $\Pi^{(1)}_{x_1}$ contained in B. So $T_1 \setminus T_0 = T_1 = \{x_1\}$. As $i = 1$, we have $|B'| \leq k|T_1 \setminus T_0| = k$. As $|B'| \geq 2^{Ckt}$, this implies $t \leq \log k/(Ck) = O(1)$. In this case, just let $k' = 1$, $y_1 = x_1$ and choose B'' to be any block in $\Pi^{(1)}_{x_1}$ contained in B other than $\{x_1\}$. By Claim 31, we have $|B|/|B''| \geq 2 = 2^{\Omega(t)}$. Thus the lemma holds.

Now assume $i > 1$. Let B_1 be the block in $\Pi'^{(1)}$ containing x_i. Consider arbitrary $x \in T_i \setminus T_{i-1}$. Let B_x be the block in $\Pi'^{(1)}$ containing x, and let B'_x be the block in $\Pi'^{(2)}$ containing (x_i, x). As $x \notin T_{i-1}$, we have $|B_x| > 1$. And as $x \in T_i$, we have $\{x\} \in \Pi^{(1)}_{x_1,\ldots,x_i} = \Pi'^{(1)}_{x_i}$. So $\{y \in S : (x_i, y) \in B'_x\} = \{x\}$. It follows that $|B'_x| = |B_1|$ by Property (P2). On the other hand, the projection $\pi_{2,2}$ maps B'_x surjectively to B_x by Property (P1). So $|B'_x| \geq |B_x|$.

We now consider the two cases $|B_x| < |B'_x|$ and $|B_x| = |B'_x|$ separately. Assume $|B'_x| > |B_x|$. Then $\Pi'^{(1)}_x$ contains a block $B''_x := \{y \in B : (x, y) \in B'_x\} \subseteq B$ of cardinality $|B'_x|/|B_x| > 1$ by Property (P2). If $|B_x| < |B|^{1/2}$, we have $|B|/|B_x| \geq |B|^{1/2} = 2^{\Omega(kt)}$. In this case, we may choose $B'' = B_x$, $k' = i - 1$ and $y_j = x_j$ for $j \in [i-1]$. On the other hand, if $|B_x| \geq |B|^{1/2}$, we have $|B|/|B''_x| \geq |B'_x|/|B''_x| = |B_x| \geq |B|^{1/2} = 2^{\Omega(kt)}$. In this case, we may choose $B'' = B''_x$, $k' = i$, $y_i = x$, and $y_j = x_j$ for $j \in [i-1]$.

So we may assume $|B_x| = |B'_x| = |B_1|$. Then $\{x\} \in \Pi'^{(1)}_{x_i}$. In fact, as $x \in T_i \setminus T_{i-1}$ is arbitrary, we may assume $|B_y| = |B'_y| = |B_1|$ for all $y \in T_i \setminus T_{i-1}$, where B_y is the block in $\Pi'^{(1)}$ containing y and B'_y is the block in $\Pi'^{(2)}$ containing (x_i, y). Consider one such y different from x and note $\{y\} \in \Pi'^{(1)}_{x_i,x}$ since $y \in T_i$. Let B^* be the block in $\Pi'^{(3)}$ containing (x_i, x, y). Then $|B^*| = |B_1|$ since $\{x\} \in \Pi'^{(1)}_{x_i}$ and $\{y\} \in \Pi'^{(1)}_{x_i,x}$. So $|B^*| = |B_x| = |B_y|$. It follows that the maps $\pi_{3,2}|_{B^*} : B^* \to B_x$ and $\pi_{3,3}|_{B^*} : B^* \to B_y$ are bijective. As $\pi_{3,3}|_{B^*} \circ (\pi_{3,2}|_{B^*})^{-1} \in \widetilde{\mathcal{M}}_{\Pi'}$ sends x to y, we have $|B_x| = |B_y|$ and $B_x \neq B_y$ by strong antisymmetry of Π'. As this holds for any distinct $x, y \in T_i \setminus T_{i-1}$, we have $|B|/|B_x| \geq |T_i \setminus T_{i-1}| = 2^{\Omega(kt)}$ for $x \in T_i \setminus T_{i-1}$. Then we may choose $B'' = B_x$ for some $x \in T_i \setminus T_{i-1}$, and let $k' = i - 1$ and $y_j = x_j$ for $j \in [i-1]$. ◀

Proof of Lemma 23. By Lemma 10 and Lemma 12, for $t \in \mathbb{N}$, the set of $x \in A$ for which there exist precisely t elements y in A satisfying $\sigma_k(y) = \sigma_k(x)$ is in $\mathcal{B}(\Pi^{(k)})$. As $A \in \Pi^{(k)}$, $\#\{y \in A : \sigma_k(y) = \sigma_k(x)\}$ is constant independent of $x \in A$. So for $x \in A' = \sigma_k(A)$, $\#\{y \in A : \sigma_k(y) = x\}$ is independent of x and equals $|A|/|A'|$.

Let $x, x' \in A$ such that $\sigma_k(x) = \sigma_k(x')$. We want to prove $x = x'$. Let T be the set of $y \in A$ satisfying $\sigma_k(y) = \sigma_k(x)$. Then $|T| = |A|/|A'|$. We also have $T \in \mathcal{B}(\Pi^{(k)}_x)$ by Lemma 10. Let B be the block in $\Pi^{(k)}_x$ containing x'. As $x' \in T$, we have $B \subseteq T$ and hence $|B| \leq |T| = |A|/|A'|$. By Lemma 14, Π_x is a strongly antisymmetric linear $(m-k)$-scheme. As $m - k > \log|A|/|A'| \geq \log|B|$, we have $B = \{x'\}$ by Lemma 16 (2).

Let B' be the block in $\Pi^{(2k)}$ containing (x, x'). Denote by $\pi_1 : V^{2k} \to V^k$ (resp. $\pi_2 : V^{2k} \to V^k$) the projection to the first (resp. last) k coordinates. Note $\pi_1, \pi_2 \in \mathcal{M}_{2k,k}$. We

have $\pi_1(B') = \pi_2(B') = A$ and $|B'| = |A||B| = |A|$. So $\pi_1|_{B'} : B' \to A$ and $\pi_2|_{B'} : B' \to A$ are bijections. Then $\pi_2|_{B'} \circ (\pi_1|_{B'})^{-1}$ is in $\widetilde{\mathcal{M}_\Pi}$ and sends x to x'. By strong antisymmetry of Π, we have $x = x'$, as desired. ◀

Proof of Lemma 24. Consider $i \in [m']$ and $B \in \Pi^{(ki)}$ such that $B \subseteq A^i$. We prove that $\sigma_k^{(i)}|_B : B \to \sigma_k^{(i)}(B)$ is bijective. Consider $\mathbf{x} = (x_1, \ldots, x_i), \mathbf{y} = (y_1, \ldots, y_i) \in B$ such that $\sigma_k^{(i)}(\mathbf{x}) = \sigma_k^{(i)}(\mathbf{y})$, i.e., $\sigma_k(x_j) = \sigma_k(y_j)$ for $j \in [i]$. As $B \subseteq A^i$, we have $x_j, y_j \in A$ for $j \in [i]$. As $\sigma_k|_A : A \to A'$ is bijective, we have $x_j = y_j$ for $j \in [i]$. So $\mathbf{x} = \mathbf{y}$, i.e., $\sigma_k^{(i)}|_B : B \to \sigma_k^{(i)}(B)$ is bijective.

It remains to prove that Π' is a well defined strongly antisymmetric linear m'-scheme on A'. Let $i \in [m']$. We first prove that $\Pi'^{(i)}$ is a well defined partition of A'^i. Note the union of the sets in $\Pi'^{(i)}$ is $\sigma_k^{(i)}(A^i) = \sigma_k(A)^i = A'^i$. To prove that $\Pi'^{(i)}$ is a partition, consider $B, B' \in \Pi^{(ki)}$ satisfying $\sigma_k^{(i)}(B) \cap \sigma_k^{(i)}(B') \neq \emptyset$. We want to show $\sigma_k^{(i)}(B) = \sigma_k^{(i)}(B')$. To see this, let T be the set of $x \in B$ for which there exists $y \in B'$ satisfying $\sigma_k^{(i)}(x) = \sigma_k^{(i)}(y)$. Then $T \in \mathcal{B}(\Pi^{(ki)})$ by Lemma 12. As $\sigma_k^{(i)}(B) \cap \sigma_k^{(i)}(B') \neq \emptyset$, we have $T \neq \emptyset$. As $T \subseteq B$ and $B \in \Pi^{(ki)}$, we have $T = B$. This implies $\sigma_k^{(i)}(B) \subseteq \sigma_k^{(i)}(B')$. Similarly, $\sigma_k^{(i)}(B') \subseteq \sigma_k^{(i)}(B)$. So $\sigma_k^{(i)}(B) = \sigma_k^{(i)}(B')$, as desired.

Consider $B \in \Pi'^{(i)}$, $B' \in \Pi'^{(i')}$ and $\tau \in \mathcal{M}_{i,i'}$ such that $\tau(B) \cap B' \neq \emptyset$. Choose $\widetilde{B} \in \Pi^{(ki)}$ and $\widetilde{B}' \in \Pi^{(ki')}$ such that $\widetilde{B} \subseteq A^i$, $\widetilde{B}' \subseteq A^{i'}$, $\sigma_k^{(i)}(\widetilde{B}) = B$ and $\sigma_k^{(i')}(\widetilde{B}') = B'$. By Property (P2) of Π, when x ranges over $\widetilde{B}$, the number of $y \in \widetilde{B}'$ satisfying $(\tau \circ \sigma_k^{(i)})(x) = \sigma_k^{(i')}(y)$ is independent of x. And this number is positive iff $(\tau \circ \sigma_k^{(i)})(x) \in \sigma_k^{(i')}(\widetilde{B}') = B'$. As $\tau(B) \cap B' \neq \emptyset$ and $\tau(B) = (\tau \circ \sigma_k^{(i)})(\widetilde{B})$, we know this number is indeed positive. So $\tau(B) \subseteq B'$. Again by Property (P2) of Π, when y ranges over $\widetilde{B}'$, the number of $x \in \widetilde{B}$ satisfying $(\tau \circ \sigma_k^{(i)})(x) = \sigma_k^{(i')}(y)$ is independent of y. So the map $\tau \circ \sigma_k^{(i)}|_{\widetilde{B}} : \widetilde{B} \to B'$ is a surjective d-to-1 map for some $d \in \mathbb{N}^+$. As $\sigma_k^{(i)}|_{\widetilde{B}} : \widetilde{B} \to B$ is bijective, we know $\tau|_B : B \to B'$ is also a surjective d-to-1 map. This proves Properties (P1) and (P2) of Π'. So Π' is a linear m'-scheme.

Now further assume $\tau|_B : B \to B'$ is bijective. We claim there exists a bijection $\tau' : \widetilde{B} \to \widetilde{B}'$ in $\widetilde{\mathcal{M}_\Pi}$ making the following diagram commute.

$$\begin{array}{ccc} \widetilde{B} & \xrightarrow{\tau'} & \widetilde{B}' \\ {\scriptstyle \sigma_k^{(i)}}\downarrow & & \downarrow{\scriptstyle \sigma_k^{(i')}} \\ B & \xrightarrow{\tau} & B' . \end{array}$$

To see this, define $\Delta := \{(x, y) \in \widetilde{B} \times \widetilde{B}' : (\tau \circ \sigma_k^{(i)})(x) = \sigma_k^{(i')}(y)\}$. Then $\Delta \in \mathcal{B}(\Pi^{(ki+ki')})$. As $\sigma_k^{(i)}|_{\widetilde{B}} : \widetilde{B} \to B$, $\sigma_k^{(i')}|_{\widetilde{B}'} : \widetilde{B}' \to B'$ and $\tau|_B : B \to B'$ are bijective, for every $x \in \widetilde{B}$, there exists unique $y \in \widetilde{B}'$ satisfying $(x, y) \in \Delta$. So $|\Delta| = |\widetilde{B}| = |\widetilde{B}'|$. Let π_1 (resp. π_2) be the projection from $V^{ki} \times V^{ki'}$ to V^{ki} (resp. $V^{ki'}$). Then π_1 (resp. π_2) maps Δ bijectively to $\widetilde{B}$ (resp. $\widetilde{B}'$). By the definition of Δ, the map $\tau' := \pi_2|_\Delta \circ (\pi_1|_\Delta)^{-1} \in \widetilde{\mathcal{M}_\Pi}$ makes the above diagram commute. This proves the claim.

By the claim just proved, every nontrivial permutation in $\widetilde{\mathcal{M}_{\Pi'}}$ lifts to a nontrivial permutation in $\widetilde{\mathcal{M}_\Pi}$. Therefore, as Π is strongly antisymmetric, so is Π'. ◀

Proof of Claim 25. Consider an arbitrary block $U \in \Pi'^{(1)}_{x_1,\ldots,x_r}$ satisfying $U \subseteq A''$. We will find $U' \in \Pi^{(k)}_y$ such that $U' \subseteq A$ and $\sigma_k(U') = U$. As $\sigma_k|_A : A \to A'$ is bijective, this implies $|U'| = |U|$. The claim follows by choosing T to be the (disjoint) union of these sets U' where U ranges over the blocks in $\Pi'^{(1)}_{x_1,\ldots,x_r}$ that are subsets of A''.

As $U \in \Pi'^{(1)}_{x_1,\ldots,x_r}$, there exists $Z \in \Pi'^{(r+1)}$ such that $U = \{z \in A' : (x_1, \ldots, x_r, z) \in Z\}$. Note $Z \subseteq A'^{r+1}$. Fix $z_0 \in U$ and choose $z_0' \in A$ such that $\sigma_k(z_0') = z_0$. Choose $\widetilde{Z} \in \Pi^{(k(r+1))}$ to be the block containing $(y_1, \ldots, y_r, z_0')$. Then $\widetilde{Z} \subseteq A^{r+1}$.

Note $\sigma_k^{(r+1)}(y_1, \ldots, y_r, z_0') = (x_1, \ldots, x_r, z_0) \in Z$. So $\sigma_k^{(r+1)}(\widetilde{Z}) \cap Z \neq \emptyset$. As $\sigma_k^{(r+1)}(\widetilde{Z}) \in \Pi'^{(r+1)}$ by the definition of Π', we have $\sigma_k^{(r+1)}(\widetilde{Z}) = Z$. Let $U' = \{z \in A : (y_1, \ldots, y_r, z) \in \widetilde{Z}\} \subseteq A$. Then $U' \in \Pi_y^{(k)}$.

It remains to prove $\sigma_k(U') = U$. Consider $z \in \sigma_k(U') \subseteq A'$ and choose $z' \in U'$ such that $z = \sigma_k(z')$. As $z' \in U'$, we have $(y_1, \ldots, y_r, z') \in \widetilde{Z}$. So $\sigma_k^{(r+1)}(y_1, \ldots, y_r, z') = (x_1, \ldots, x_r, z) \in Z$. Therefore $z \in U$. This proves $\sigma_k(U') \subseteq U$.

Now consider $z \in U$. Then $(x_1, \ldots, x_r, z) \in Z$. As $\sigma_k^{(r+1)}(\widetilde{Z}) = Z$, there exists $(y_1', \ldots, y_r', z') \in \widetilde{Z}$ such that $\sigma_k^{(r+1)}(y_1', \ldots, y_r', z') = (x_1, \ldots, x_r, z)$, i.e., $\sigma_k(z') = z$ and $\sigma_k(y_i') = x_i = \sigma_k(y_i)$ for $i \in [r]$. As $\sigma_k|_A : A \to A'$ is bijective, we have $y_i' = y_i$ for $i \in [r]$. So $(y_1, \ldots, y_r, z') \in \widetilde{Z}$. It follows that $z' \in U'$. So $z = \sigma_k(z') \subseteq \sigma_k(U')$. This proves $\sigma_k(U') \supseteq U$. Therefore $\sigma_k(U') = U$. ◀

D Proof of Lemma 21

We prove Lemma 21 in this section, which addresses the case that $B \in \Pi^{(1)}$ is dense in $\langle B \rangle$.

D.1 Additional Notations and Preliminaries.

We first introduce additional notations and preliminaries that are used in the proof of Lemma 21.

Fourier analysis on finite abelian groups. For a finite abelian group A, write $\widehat{A}$ for the dual group $\mathrm{Hom}(A, \mathbb{C}^\times)$. Elements in $\widehat{A}$ are called *characters* of A. The complex conjugate $\overline{\chi}$ of a character χ is again a character. For a function $f : A \to \mathbb{C}$ and a character $\chi \in \widehat{A}$, define the *χ-th Fourier coefficient* $\widehat{f}(\chi) := \mathbb{E}_{a \in A}[f(a)\overline{\chi(a)}]$. Then $f = \sum_{\chi \in \widehat{A}} \widehat{f}(\chi)\chi$. We also have *Parseval's identity*:

$$\mathop{\mathbb{E}}_{a \in A}\left[|f(a)|^2\right] = \sum_{\chi \in \widehat{A}} |\widehat{f}(\chi)|^2.$$

Additive combinatorics. For $A \subseteq V$, write $\mathbb{F}A$ for the cone $\{ca : c \in \mathbb{F}, a \in A\} \subseteq V$. Let $A^{\pm} := A \cup (-A) \cup \{0\} \subseteq \mathbb{F}A$. Define $h(A)$ to be smallest $k \in \mathbb{N}^+$ such that $kA^{\pm} = \langle A \rangle$. The problem of bounding $h(A)$ in terms of $\mu(A)$ has been studied in [19, 24]. In particular, the following bound was obtained in [19].

▶ **Theorem 32** ([19, Lemma 3]). $h(A) \leq \max\left\{2, \lfloor \frac{3}{2\mu(A)} \rfloor\right\}$.

For $A \subseteq V$, the *additive energy* $E(A)$ of A is defined by:

$$\begin{aligned} E(A) :&= \#\{(a_1, a_2, a_3, a_4) \in A^4 : a_1 + a_2 = a_3 + a_4\} \\ &= \#\{(a_1, a_2, a_3, a_4) \in A^4 : a_1 - a_3 = a_4 - a_2\}. \end{aligned}$$

If $|A + A|/|A|$ is small, then $E(A)$ is large, as the map $A \times A \to A + A$ sending (a, b) to $a + b$ has a lot of "collisions". The converse of this statement is false. Nevertheless, the famous Balog-Szemerédi-Gowers Theorem [4, 14] states that if $E(A)$ is large enough, then there always exists a dense subset $A' \subseteq A$ such that $|A' + A'|/|A'|$ is small. We need the following variant of this theorem tailored to linear m-schemes:

▶ **Theorem 33** (Balog-Szemerédi-Gowers Theorem for linear m-schemes). *Let $m \geq 4$. Let Π be a linear m-scheme and $B \in \Pi^{(1)}$ such that $E(B) \geq \gamma|B|^3$, where $\gamma > 0$. Then there exists $B' \subseteq B$ such that $|B'| \geq \gamma|B|/3$ and $|B' - B'| < 2^{17}\gamma^{-9}|B|$. Moreover, B' can be chosen such that $B' \in \mathcal{B}(\Pi_x^{(1)})$ for some $x \in B$.*

Theorem 33 basically follows from the usual form of the Balog-Szemerédi-Gowers Theorem except the last claim that we may assume $B' \in \mathcal{B}(\Pi_x^{(1)})$ for some $x \in B$. This claim too can be verified by following Gowers' proof in [14]. For the sake of completeness, we present a proof following [14], where some steps are simplified using properties of linear m-schemes.

Proof of Theorem 33. We will prove that there exist $x \in B$ and $B' \in \Pi_x^{(1)}$ such that $B' \subseteq B$, $|B'| \geq \gamma|B|/3$, and for any $a_1, a_2 \in B'$, the number of solutions of the equation

$$a_1 - a_2 = (x_1 - y_1) - (x_2 - y_2) - (x_3 - y_3) + (x_4 - y_4)$$

in the variables $x_i, y_i \in B$ $(i = 1, 2, 3, 4)$ is greater than $2^{-17}\gamma^9|B|^7$. Note that this implies $|B' - B'| < |B|^8/(2^{-17}\gamma^9|B|^7) = 2^{17}\gamma^{-9}|B|$, as claimed.

For $z \in B - B$, write $\nu^-(z)$ for the number of $(x, y) \in B \times B$ satisfying $x - y = z$. Then

$$\sum_{z \in B-B} \nu^-(z) = |B|^2 \quad \text{and} \quad \sum_{z \in B-B} \nu^-(z)^2 = E(B).$$

Let $T := \{z \in B - B : \nu^-(z) \geq \gamma|B|/2\}$. For $x \in B$, let $N(x) := \{y \in B : x - y \in T\}$. For $y \in B$, let $N'(y) := \{x \in B : y \in N(x)\} = \{x \in B : x - y \in T\}$. Note

$$\sum_{z \in T} \nu^-(z)^2 = \sum_{z \in B-B} \nu^-(z)^2 - \sum_{z \in (B-B)\setminus T} \nu^-(z)^2 \geq E(B) - |B|^2 \cdot \gamma|B|/2 \geq \gamma|B|^3/2. \quad (4)$$

On the other hand,

$$\sum_{x \in B} |N(x)| = \sum_{x \in B} |N'(x)| = \sum_{z \in T} \nu^-(z) \geq \sum_{z \in T} \nu^-(z)^2/|B|. \quad (5)$$

By (4) and (5), we have $\sum_{x \in B} |N(x)| = \sum_{x \in B} |N'(x)| \geq \gamma|B|^2/2$. Note $N(x), N'(x) \in \mathcal{B}(\Pi_x^{(1)})$ for $x \in B$ by Lemma 12. By Property (P2) of Π, $|N(x)|$ (resp. $|N'(x)|$) is constant when x ranges over B. Therefore, $|N(x)| = |N'(x)| \geq \gamma|B|/2$ for all $x \in B$.

Let N be the cardinality of the sets $N(x)$ and $N'(x)$. Then $N \geq \gamma|B|/2$. For $x \in B$, let $M(x)$ be the number of pairs $(y, z) \in N'(x) \times N'(x)$ satisfying $|N(y) \cap N(z)| \leq \gamma^2|B|/36$. By Property (P2) of Π, $M(x)$ is independent of $x \in B$. Choose arbitrary $x_0 \in B$. Note that for $x, y \in B$, we have $x \in N(y)$ iff $y \in N'(x)$. Therefore

$$\begin{aligned} M(x_0) &= \sum_{x \in B} M(x)/|B| = \sum_{x \in B} \sum_{\substack{y,z \in N'(x) \\ |N(y)\cap N(z)| \leq \gamma^2|B|/36}} 1/|B| \\ &= \sum_{\substack{y,z \in B \\ |N(y)\cap N(z)| \leq \gamma^2|B|/36}} \sum_{x \in N(y)\cap N(z)} 1/|B| \leq \gamma^2|B|^2/36 \leq N^2/9. \end{aligned} \quad (6)$$

Consider the undirected graph G on the vertex set $N'(x_0)$ such that $(y, z) \in N'(x_0) \times N'(x_0)$ is an edge in G iff $|N(y) \cap N(z)| \leq \gamma^2|B|/36$. By (6), the average degree of G is at most $N/9$. By Markov's inequality, at most $(1/3)$-fraction of vertices $y \in N'(x_0)$ satisfy $\deg(y) \geq N/3$. Let

$$B' := \{y \in N'(x_0) : \deg(y) \leq N/3\} \subseteq B.$$

Then $|B'| \geq 2N/3 \geq \gamma|B|/3$. Also note $B' \in \mathcal{B}(\Pi^{(1)}_{x_0})$ by Lemma 12.

By definition, for all $y \in B'$, we have

$$\#\{z \in N'(x_0) : |N(y) \cap N(z)| \leq \gamma^2|B|/36\} \leq N/3.$$

Consider arbitrary $a_1, a_2 \in B'$. By the union bound, we have

$$\#\{z \in N'(x_0) : |N(a_i) \cap N(z)| > \gamma^2|B|/36 \text{ for } i = 1, 2\} \geq N - 2(N/3) \geq \gamma|B|/6. \tag{7}$$

Consider any $z \in N'(x_0)$ satisfying $|N(a_i) \cap N(z)| > \gamma^2|B|/36$ for $i = 1, 2$. For any $w \in N(a_1) \cap N(z)$, we have $\nu^-(a_1 - w), \nu^-(z - w) \geq \gamma|B|/2$, yielding at least $(\gamma|B|/2)^2$ representations of $a_1 - z$ of the form

$$a_1 - z = (x_1 - y_1) - (x_2 - y_2)$$

such that $x_1, y_1, x_2, y_2 \in B$, $x_1 - y_1 = a_1 - w$, and $y_2 - x_2 = z - w$. As the number of choices for $w \in N(a_1) \cap N(z)$ is at least $\gamma^2|B|/36$, there are at least $(\gamma|B|/2)^2 \cdot \gamma^2|B|/36 = \gamma^4|B|^3/144$ representations $a_1 - z = (x_1 - y_1) - (x_2 - y_2)$ where $x_1, y_1, x_2, y_2 \in B$. (Note different choices of w yield different representations as $w = a_1 - x_1 + y_1$ can be recovered from a representation.) Similarly, there are at least $\gamma^4|B|^3/144$ representations $a_2 - z = (x_3 - y_3) - (x_4 - y_4)$ where $x_3, y_3, x_4, y_4 \in B$. Combining, we obtain at least $(\gamma^4|B|^3/144)^2$ representations of $a_1 - a_2$ of the form $a_1 - a_2 = ((x_1 - y_1) - (x_2 - y_2)) - ((x_3 - y_3) - (x_4 - y_4))$ using each z. By (7), there are at least $\gamma|B|/6$ choices of z, yielding at least $\gamma|B|/6 \cdot (\gamma^4|B|^3/144)^2 > 2^{-17}\gamma^9|B|^7$ representations of $a_1 - a_2$ of the form

$$a_1 - a_2 = (x_1 - y_1) - (x_2 - y_2) - (x_3 - y_3) + (x_4 - y_4).$$

where $x_i, y_i \in B$ for $i = 1, 2, 3, 4$. (Again, different choices of z yield different representations as $z = a_1 - (x_1 - y_1) + (x_2 - y_2)$ can be recovered from a representation.) This completes the proof. ◀

D.2 Constructible Sets

We define and discuss the notion of *constructible sets* in this subsection, which will be useful later.

▶ **Definition 34** (constructible set)**.** *Let Π be a linear m-scheme on S, and $k \in [m]$. Define*

$$\mathcal{S}_{\Pi,k} := \{\tau(B) : B \in \Pi^{(k)}, \tau \in \mathcal{M}_{k,1}\}.$$

We say a subset T of V is (Π, k)-constructible *if $T \in \mathcal{B}(\mathcal{S}_{\Pi,k})$, i.e., T is a union of sets $T_1, \ldots, T_r$ where each T_i is the image of a block $B_i \in \Pi^{(k)}$ under a map $\tau_i \in \mathcal{M}_{k,1}$.*

▶ **Lemma 35.** *We have*

1. *For $T \in \mathcal{B}(\mathcal{S}_{\Pi,k})$, $T \cap S \in \mathcal{B}(\Pi^{(1)})$.*
2. *Suppose $T \in \mathcal{B}(\mathcal{S}_{\Pi,k})$ and $T' \in \mathcal{B}(\mathcal{S}_{\Pi,k'})$ where $k + k' \leq m$. Then $T \cap T', T \setminus T' \in \mathcal{B}(\mathcal{S}_{\Pi,k})$.*

Proof. The first claim holds by Lemma 12 (3). For the second claim, it suffices to show that for $B \in \Pi^{(k)}$, $B' \in \Pi^{(k')}$, $\tau \in \mathcal{M}_{k,1}$ and $\tau' \in \mathcal{M}_{k',1}$, we have $\tau(B) \cap \tau'(B'), \tau(B) \setminus \tau'(B') \in \mathcal{B}(\mathcal{S}_{\Pi,k})$. To see this, let $\Delta = \{(x, y) \in B \times B' : \tau(x) = \tau'(y)\}$. Then $\Delta \in \mathcal{B}(\Pi^{(k+k')})$ by Lemma 10. Let $B'' = \{x \in B : \exists y \in B' \text{ such that } (x, y) \in \Delta\}$. Then $B'', B \setminus B'' \in \mathcal{B}(\Pi^{(k)})$ by Lemma 12. Note $\tau(B) \cap \tau'(B') = \tau(B'')$ and $\tau(B) \setminus \tau'(B') = \tau(B \setminus B'')$. So $\tau(B) \cap \tau'(B'), \tau(B) \setminus \tau'(B') \in \mathcal{B}(\mathcal{S}_{\Pi,k})$. ◀

We also need the following technical lemma.

▶ **Lemma 36.** *Let W and W' be linear subspaces of V such that $W \subseteq W'$. Let $d = \dim W' - \dim W$. Suppose W is (Π, k)-constructible for some $k \in [m]$. Also suppose $W' \subseteq W + t(\mathbb{F}S)$ for some $t \in \mathbb{N}$ satisfying $k + 2dt \leq m$. Then there exists $x \in S^{dt}$ such that W' is $(\Pi_x, k + dt)$-constructible.*

Proof. Choose $x_1, \ldots, x_d \in W'$ such that $W' = W + \sum_{i=1}^{d} \mathbb{F}x_i$. As $W' \subseteq W + t(\mathbb{F}S)$, we may assume $x_1, \ldots, x_d \in t(\mathbb{F}S)$. For $i \in [d]$, write $x_i = \sum_{j=1}^{t} c_{i,j}x_{i,j}$ for some $c_{i,j} \in \mathbb{F}$ and $x_{i,j} \in S$. Let $x = (x_{i,j})_{i\in[d],j\in[t]} \in S^{dt}$.

Consider $B \in \Pi^{(k)}$ and $\tau \in \mathcal{M}_{k,1}$, so that $\tau(B) \in \mathcal{S}_{\Pi,k}$. Let $B' = B \times \{x_{1,1}\} \times \{x_{1,2}\} \times \cdots \times \{x_{d,t}\} \in \mathcal{B}(\Pi_x^{(k+dt)})$. For $s = (s_1, \ldots, s_d) \in \mathbb{F}^d$, let $\tau_s : V^k \times V^{dt} \to V$ be the map sending $(y, (z_{i,j})_{i\in[d],j\in[t]})$ to $\tau(y) + \sum_{i=1}^{d} s_i \cdot \left(\sum_{j=1}^{t} c_{i,j}z_{i,j}\right)$. We have $\tau_s \in \mathcal{M}_{k+dt,1}$ for $s \in \mathbb{F}^d$. Then

$$\tau(B) + \sum_{i=1}^{d} \mathbb{F}x_i = \bigcup_{s\in\mathbb{F}^d} \tau_s(B') \in \mathcal{B}(\mathcal{S}_{\Pi_x,k+dt}).$$

As W is a union of sets of the form $\tau(B)$ with $B \in \Pi^{(k)}$ and $\tau \in \mathcal{M}_{k,1}$, we have $W' = W + \sum_{i=1}^{d} \mathbb{F}x_i \in \mathcal{B}(\mathcal{S}_{\Pi_x,k+dt})$. ◀

D.3 The Decomposition Theorem

As mentioned before, one key idea in the proof is reducing the density of B. We know that if $|B| > 1$, then the set $B \setminus \{x\}$ contains two different blocks $B', B'' \in \Pi_x^{(1)}$ of equal size (see the proof of Claim 31). Suppose $\langle B'\rangle = \langle B''\rangle = \langle B\rangle$. Then

$$\mu(B') = |B'|/|\langle B'\rangle| \leq \frac{1}{2}|B|/|\langle B\rangle| = \mu(B)/2.$$

In this case, replacing Π by Π_x and B by B' reduces the density by at least a factor of two. Continuing this process, we would obtain a block of density at most $\exp(-k)$ in k steps.

Unfortunately, we do not know if $\langle B'\rangle = \langle B''\rangle = \langle B\rangle$ always holds. If $\langle B'\rangle \subsetneq \langle B\rangle$, then it might happen that $\mu(B') \gg \mu(B)$. Note that if this occurs, then B is "overrepresented" in the proper subspace $\langle B'\rangle$, i.e., $\mu_{\langle B'\rangle}(B) \geq \mu(B') \gg \mu(B)$.

To address this problem, we want to find a subspace $W \subseteq \langle B\rangle$ such that B is "psedo-random" within W in the sense that $\mu_{W\cap\langle B'\rangle}(B) \approx \mu_W(B)$. Then, by restricting to the subspace W, we can make sure that overrepresentation does not occur.

How do we find W? Consider the case $\mu_{\langle B'\rangle}(B) \gg \mu(B)$ and assume $\langle B'\rangle$ is a hyperplane of $\langle B\rangle$ for simplicity. It is easy to see that the characteristic function 1_B must have a non-negligible correlation with some nontrivial character $\chi \in \widehat{\langle B\rangle}$ vanishing on $\langle B'\rangle$, i.e., $|\widehat{1}_B(\chi)| \geq \epsilon$ where $\epsilon > 0$ is non-negligible. So, we could choose W to be the intersection of $\ker(\chi)$ where χ ranges over the set of nontrivial characters satisfying $|\widehat{1}_B(\chi)| \geq \epsilon$. Then restricting to the subspace W "quotients out" these characters.

However, there are two problems with this idea. The first one is that we need to make sure restricting to W maintains the linear m-scheme structure. This is solved by considering only the nontrivial characters whose kernels are constructible sets instead of all characters.

The second problem is that the set $W \cap B$ may simply be empty, in which case the statement $\mu_{W\cap\langle B'\rangle}(B) \approx \mu_W(B)$ is trivially true but no longer useful. In this case, instead of restricting to the subspace W, we restrict to $W' = W + \mathbb{F}x$ for some $x \in B$. As $x \in B$ may vary, we actually find a collection of subspaces W_i of $\langle B\rangle$ instead of a single subspace.

The main result of this subsection is a decomposition theorem that allows us to find the subspaces W_i. To formally state this result, we need the following definitions.

▶ **Definition 37.** *Let Π be a linear m-scheme on S. Let $B \in \Pi^{(1)}$ and $1 \le k \le m/2$. define $\mathcal{W}_{\Pi,k,B}$ to be the set of subspaces $W \subseteq \langle B \rangle$ such that (1) the codimension of W in $\langle B \rangle$ is at most k, and (2) W is (Π_x, k)-constructible for some $x \in S^k$.*

▶ **Definition 38.** *Let Π be a linear m-scheme on S. Let $B \in \Pi^{(1)}$, $1 \le k \le m/2$, and $0 < \epsilon < 1$. Define $\mathcal{X}_{\Pi,k,B,\epsilon}$ to be the set of nontrivial characters $\chi \in \widehat{\langle B \rangle}$ such that $|\widehat{1_B}(\chi)| \ge \epsilon$ and $\ker(\chi) \in \mathcal{W}_{\Pi,k,B}$.*

The next lemma states that if B is not pseudorandom against a subspace $W \in \mathcal{W}_{\Pi,k,B}$, then there exists a nontrivial character χ such that $|\widehat{1}_B(\chi)|$ is non-negligible and $\ker(\chi)$ is constructible.

▶ **Lemma 39.** *Let Π be a linear m-scheme on S. Let $B \in \Pi^{(1)}$, $1 \le k \le m/2$, and $0 < \epsilon < 1$. Let $t = \lfloor \frac{3}{2\mu(B)} \rfloor + 1$, $k' = k(t+1)$ and $\epsilon' = \epsilon/\ell^k$ (recall $\ell = \mathrm{char}(\mathbb{F}) = |\mathbb{F}|$). Suppose $m \ge 2k'$. Then one of the following is true:*
1. *$|\mu_W(B) - \mu(B)| \le \epsilon$ for all $W \in \mathcal{W}_{\Pi,k,B}$.*
2. *$\mathcal{X}_{\Pi,k',B,\epsilon'} \ne \emptyset$.*

Proof. Suppose (1) does not hold. Choose $W \in \mathcal{W}_{\Pi,k,B}$ such that $|\mu_W(B) - \mu(B)| > \epsilon$. Let $G \subseteq \widehat{\langle B \rangle}$ be the subgroup of characters χ vanishing on W. Then $|G| = |V|/|W| \le \ell^k$. Let $1_W : \langle B \rangle \to \mathbb{C}$ be the characteristic function of W. Note $\widehat{1_W}(\chi) = |W|/|\langle B \rangle|$ for $\chi \in G$ and $\widehat{1_W}(\chi) = 0$ for $\chi \in \widehat{\langle B \rangle} \setminus G$. So

$$1_W = |W|/|\langle B \rangle| \cdot \sum_{\chi \in G} \chi. \tag{8}$$

Also note for $\chi \in \widehat{\langle B \rangle}$, we have

$$\mathop{\mathbb{E}}_{a \in B}[\chi(a)] = \mu(B)^{-1} \mathop{\mathbb{E}}_{a \in \langle B \rangle}[1_B(a)\chi(a)] = \mu(B)^{-1} \widehat{1_B}(\overline{\chi}). \tag{9}$$

Denote by χ_0 the trivial character in $\widehat{\langle B \rangle}$. Then we have

$$\begin{aligned} \mu_W(B) &= \sum_{a \in B} 1_W(a)/|W| \overset{(8)}{=} \sum_{\chi \in G} \sum_{a \in B} \chi(a)/|\langle B \rangle| \\ &= \left(\sum_{\chi \in G} \mathop{\mathbb{E}}_{a \in B}[\chi(a)] \right) \cdot \mu(B) \overset{(9)}{=} \mu(B) + \sum_{\chi \in G \setminus \{\chi_0\}} \widehat{1_B}(\overline{\chi}). \end{aligned} \tag{10}$$

As $|\mu_W(B) - \mu(B)| > \epsilon$, there exists $\chi^* \in G \setminus \{\chi_0\}$ such that $|\widehat{1_B}(\chi^*)| = |\widehat{1_B}(\overline{\chi^*})| \ge \epsilon/|G| \ge \epsilon'$ (the first equality holds as 1_B is real-valued).

As $\chi^* \in G$, we have $W \subseteq \ker(\chi^*)$. Note $\dim \ker(\chi^*) - \dim W \le \dim \langle B \rangle - \dim W \le k$. Also note $\ker(\chi^*) \subseteq \langle B \rangle \subseteq t(\mathbb{F}B)$ by Theorem 32. As $W \in \mathcal{W}_{\Pi,k,B}$, we know W is (Π_x, k)-constructible for some $x \in S^k$. Then by Lemma 36, $\ker(\chi^*)$ is $((\Pi_x)_{x'}, k + kt)$-constructible for some $x' \in S^{kt}$. It follows that $\ker(\chi^*) \in \mathcal{W}_{\Pi,k',B}$. So $\chi^* \in \mathcal{X}_{\Pi,k',B,\epsilon'}$ and hence $\mathcal{X}_{\Pi,k',B,\epsilon'} \ne \emptyset$. ◀

Now we are ready to state and prove the *decomposition theorem*.

▶ **Theorem 40** (decomposition theorem). *Let Π be a linear m-scheme on S. Let $B \in \Pi^{(1)}$, $1 \le k' \le m/4$, and $0 < \epsilon' < 1$. Let $t = \lfloor \frac{3}{2\mu(B)} \rfloor + 1$. Suppose $m \ge 2t+2$ and $\mathcal{X}_{\Pi,k',B,\epsilon'} \ne \emptyset$. Let $H = \bigcap_{\chi \in \mathcal{X}_{\Pi,k',B,\epsilon'}} \ker(\chi)$, and let $\mathcal{C}$ be the set of subspaces $\{H + \mathbb{F}x : x \in B\}$. Then we have:*

1. *$H \in \mathcal{B}(\mathcal{S}_{\Pi,t})$, i.e., H is (Π, t)-constructible.*
2. *$B \cap H = \emptyset$.*
3. *H is a hyperplane of every $W \in \mathcal{C}$.*
4. *$W \cap W' = H$ for distinct $W, W' \in \mathcal{C}$. In particular, $\{B \cap W : W \in \mathcal{C}\}$ is a partition of B by (2).*
5. *The sets $B \cap W$ have equal size, where W ranges over $\mathcal{C}$.*
6. *$|\mathcal{C}| \le \ell^{1/\epsilon'^2}$.*
7. *Let $W \in \mathcal{C}$ and $W' \in \mathcal{W}_{\Pi,k'',B}$ where $1 \le k'' \le m/2$. Let d be the codimension of $W \cap W'$ in $\langle B \rangle$. Suppose $k' \ge k'' + dt + 1$. Then either $|\mu_{W \cap W'}(B) - \mu_W(B)| \le \ell^d \epsilon'$ or $\mu_{W \cap W'}(B) = 0$. The latter case occurs only if $W \cap W' \subseteq H$.*

By Lemma 39, if B is not pseudorandom against some subspace in $\mathcal{W}_{\Pi,k,B}$, i.e., $|\mu_W(B) - \mu(B)| > \epsilon$ for some $W \in \mathcal{W}_{\Pi,k,B}$, then $\mathcal{X}_{\Pi,k',B,\epsilon'}$ is nonempty. Then we can find a collection of subspaces $\mathcal{C} = \{H + \mathbb{F}x : x \in B\}$, where $H = \bigcap_{\chi \in \mathcal{X}_{\Pi,k',B,\epsilon'}} \ker(\chi)$. Theorem 40 (7) then states that, by restricting to each $W \in \mathcal{C}$, B becomes pseudorandom in the weaker sense that for small enough k'' and $W' \in \mathcal{W}_{\Pi,k'',B}$ satisfying $W \cap W' \not\subseteq H$, we have $\mu_{W \cap W'}(B) \approx \mu_W(B)$ (however, if $W \cap W' \subseteq H$, we would have $\mu_{W \cap W'}(B) = 0$).

Moreover, the set H is constructible (Theorem 40 (1)) and is a common hyperplane of $W \in \mathcal{C}$ (Theorem 40 (3)). It is also the common intersection of $W \in \mathcal{C}$ (Theorem 40 (4)). So the subspaces $W \in \mathcal{C}$ form a "sunflower" where H is the "kernel". The set B is evenly distributed on the "leaves" of the sunflower (Theorem 40 (2), (4) and (5)). Finally, we have an upper bound for the number of leaves (Theorem 40 (6)).

Proof of Theorem 40. (1): For $\chi \in \mathcal{X}_{\Pi,k',B,\epsilon'}$, we will find a subspace $H_\chi \subseteq \langle B \rangle$ satisfying $H_\chi \in \mathcal{B}(\mathcal{S}_{\Pi,t})$ and $H \subseteq H_\chi \subseteq \ker(\chi)$. Then $H = \bigcap_{\chi \in \mathcal{X}_{\Pi,k',B,\epsilon'}} H_\chi$ since

$$H \subseteq \bigcap_{\chi \in \mathcal{X}_{\Pi,k',B,\epsilon'}} H_\chi \subseteq \bigcap_{\chi \in \mathcal{X}_{\Pi,k',B,\epsilon'}} \ker(\chi) = H.$$

As $\mathcal{B}(\mathcal{S}_{\Pi,t})$ is closed under intersection by Lemma 35 (2), we would have $H \in \mathcal{B}(\mathcal{S}_{\Pi,t})$. So it remains to find H_χ for $\chi \in \mathcal{X}_{\Pi,k',B,\epsilon'}$.

Consider arbitrary $\chi \in \mathcal{X}_{\Pi,k',B,\epsilon'}$. As $\ker(\chi) \in \mathcal{W}_{\Pi,k',B}$, there exist $x = (x_1, \ldots, x_{k'}) \in S^{k'}$, $s \in \mathbb{N}^+$, $B_1, \ldots, B_s \in \Pi_x^{(k')}$ and $\tau_1, \ldots, \tau_s \in \mathcal{M}_{k',1}$ such that $\ker(\chi) = \bigcup_{i=1}^s \tau_i(B_i)$. We may assume the sets $\tau_i(B_i)$ are disjoint by Lemma 35 (2). For $i \in [s]$, let B_i' be the block in $\Pi^{(2k')}$ satisfying $B_i = \{y \in S^{k'} : (x, y) \in B_i'\}$, which uniquely exists since $B_i \in \Pi_x^{(k')}$. Let B^* be the block in $\Pi^{(k')}$ containing x. For $i \in [s]$ and $z \in B^*$, let $B_{i,z} = \{y \in S^{k'} : (z, y) \in B_i'\} \in \Pi_z^{(k')}$, so that $B_{i,x} = B_i$. Finally, choose $u \in B \setminus \ker(\chi)$, and let B^{**} be the block in $\Pi^{(k'+1)}$ containing (x, u).

We know $\ker(\chi) = \bigcup_{i=1}^s \tau_i(B_i)$. The idea is showing that for each $z \in B^*$, there exists a character $\chi_z \in \mathcal{X}_{\Pi,k',B,\epsilon'}$ such that $\ker(\chi_z) = \bigcup_{i=1}^s \tau_i(B_{i,z})$, and $\chi_x = \chi$. Then we can choose $H_\chi = \bigcap_{z \in \mathcal{B}^*} \ker(\chi_z)$. To achieve this, we need the following claim.

▷ Claim 41. We have:

(a) For distinct $i, j \in [s]$ and $z \in B^*$, $\tau_i(B_{i,z}) \cap \tau_j(B_{j,z}) = \emptyset$.

(b) For $i \in [s]$, $|\tau_i(B_{i,z})|$ is independent of $z \in B^*$.

(c) For $i, j \in [s]$, the number of $(a, b) \in B_{i,z} \times B_{j,z}$ satisfying $\tau_i(B_{i,z}) - \tau_j(B_{j,z}) \in \bigcup_{k=1}^{s} \tau_k(B_{k,z})$ is independent of $z \in B^*$.

(d) For all $(z, w) \in B^{**}$ where $z \in S^k$ and $w \in S$, we have $w \notin \bigcup_{i=1}^{s} \tau_i(B_{i,z})$.

(e) For $i \in [s]$ and $c \in \mathbb{F}$, $|B \cap (\tau_i(B_{i,z}) + cw)|$ is independent of $(z, w) \in \mathcal{B}^{**}$.

Proof of Claim 41. (a): Let $i, j \in [s]$ such that $i \neq j$. By Property (P2) of Π, the number of $(a, b) \in S^{k'} \times S^{k'}$ satisfying $(z, a) \in B'_i$, $(z, b) \in B'_j$ and $\tau_i(a) = \tau_j(b)$ is independent of $z \in B^*$. For each z, this number equals zero iff $\tau_i(B_{i,z}) \cap \tau_j(B_{j,z}) = \emptyset$. As $\tau_i(B_i) \cap \tau_j(B_j) = \emptyset$, we have $\tau_i(B_{i,z}) \cap \tau_j(B_{j,z}) = \emptyset$ for $z \in B^*$.

(b): Let $i \in [s]$. For $d \in \mathbb{N}^+$, let $B'_{i,d}$ be the set of $(z, y) \in B'_i$ satisfying

$$\#\{y' \in S^{k'} : (z, y') \in B'_i \text{ and } \tau_i(y') = \tau_i(y)\} = d.$$

By Lemma 12, we have $B'_{i,d} \in \mathcal{B}(\Pi^{(2k')})$ for $d \in \mathbb{N}^+$. As $B'_i \in \Pi^{(2k')}$ and $B'_{i,d} \subseteq B'_i$ for $d \in \mathbb{N}^+$, we have $B'_i = B'_{i,d_0}$ for some $d_0 \in \mathbb{N}^+$. This means for all $z \in B^*$, the map $\tau_i|_{B_{i,z}} : B_{i,z} \to \tau_i(B_{i,z})$ is a d_0-to-1 map. By Property (P2) of Π, $|B_{i,z}|$ is independent of $z \in B^*$. So $|\tau_i(B_{i,z})| = |B_{i,z}|/d_0$ is also independent of $z \in B^*$.

(c): Let $i, j \in [s]$. For $k \in [s]$, define

$$T_k = \{(z, a, b, c) \in (S^{k'})^4 : (z, c) \in B'_k \text{ and } \tau_i(a) - \tau_j(b) = \tau_k(c)\}.$$

Then $T_k \in \mathcal{B}(\Pi^{(4k')})$ for $k \in [s]$. Let $T = \bigcup_{k \in [s]} T_k \in \mathcal{B}(\Pi^{(4k')})$. By Lemma 12 and Property (P2) of Π, the number

$$\#\left\{(a, b) \in S^{k'} \times S^{k'} : \begin{array}{l}(z, a) \in B'_i, (z, b) \in B'_j, \text{and} \\ \exists\, c \in S^{k'}\ (z, a, b, c) \in T\end{array}\right\}$$

is independent of $z \in B^*$. This is precisely the number of $(a, b) \in B_{i,z} \times B_{j,z}$ satisfying $\tau_i(B_{i,z}) - \tau_j(B_{j,z}) \in \bigcup_{k=1}^{s} \tau_k(B_{k,z})$.

(d): By Property (P2) of Π, for $i \in [s]$, the number of $a \in S^{k'}$ satisfying $(z, a) \in B'_i$ and $w = \tau_i(a)$ is independent of $(z, w) \in B^{**}$. This number equals zero for all $i \in [s]$ iff $w \notin \bigcup_{i=1}^{s} \tau_i(B_{i,z})$. As $(x, u) \in B^{**}$ and $u \notin \bigcup_{i=1}^{s} \tau_i(B_i)$, we have $w \notin \bigcup_{i=1}^{s} \tau_i(B_{i,z})$ for $(z, w) \in B^{**}$.

(e): Let $i \in [s]$ and $c \in \mathbb{F}$. By Lemma 12 and Property (P2) of Π, the number

$$\#\{a \in B : \exists\, y \in S^{k'} \text{ satisfying } (z, y) \in B'_i \text{ and } a = \tau_i(y) + cw\}$$

is independent of $(z, w) \in B^{**}$. This number is precisely $|B \cap (\tau_i(B_{i,z}) + cw)|$. ◀

Let $W_z = \bigcup_{i=1}^{s} \tau_i(B_{i,z})$ for $z \in B^*$. Note $W_x = \ker(\chi)$. By Claim 41 (a) and (b), $|W_z|$ is independent of $z \in B^*$. By Claim 41 (c), for $i, j \in [s]$, the number of $(a, b) \in B_{i,z} \times B_{j,z}$ satisfying $\tau_i(B_{i,z}) - \tau_j(B_{j,z}) \in W_z$ is independent of $z \in B^*$. This number attains the maximum possible value $|B_{i,z}| \times |B_{j,z}|$ for all $i, j \in [s]$ iff $W_z - W_z \subseteq W_z$, or equivalently, W_z is an abelian subgroup of $\langle B \rangle$. As $W_x = \ker(\chi)$ is a hyperplane of $\langle B \rangle$ and $\mathbb{F}$ is a prime field, we know W_z is a hyperplane of $\langle B \rangle$ for all $z \in B^*$.

Choose $u_z \in S$ for each $z \in B^*$ such that $(z, u_z) \in B^{**}$ and $u_x = u$ (such u_z exists by Property (P2) of Π). For $z \in B^*$, we know $u_z \notin W_z$ and hence $W_z + \mathbb{F}u_z = \langle B \rangle$ by Claim 41 (d). For $z \in B^*$, let χ_z be the unique character in $\widehat{\langle B \rangle}$ satisfying $W_z \subseteq \ker(\chi_z)$ and

$\chi_z(u_z) = \chi(u)$. In particular, $\chi_x = \chi$. Note

$$\widehat{1_B}(\chi_z) = \mathop{\mathbb{E}}_{a\in\langle B\rangle}\left[1_B(a)\overline{\chi_z(a)}\right] = |\langle B\rangle|^{-1}\left(\sum_{c\in\mathbb{F}}|B\cap(W_z+cu_z)|\cdot\overline{\chi_z(cu_z)}\right)$$
$$= |\langle B\rangle|^{-1}\left(\sum_{c\in\mathbb{F}}|B\cap(W_z+cu_z)|\cdot\overline{\chi(cu)}\right).$$

By Claim 41 (b) and (e), $|B\cap(W_z+cu_z)|$ is independent of $z\in B^*$. It follows that $|\widehat{1_B}(\chi_z)| = |\widehat{1_B}(\chi)| \geq \epsilon'$ for all $z\in B^*$. Also note $W_z = \bigcup_{i=1}^s \tau_i(B_{i,z}) \in \mathcal{W}_{\Pi,k',B}$. By definition, we have $\chi_z \in \mathcal{X}_{\Pi,k',B,\epsilon'}$ for $z\in B^*$.

For $i\in[s]$, let

$$U_i = \left\{a\in S^{k'}: \begin{array}{l}\forall\, z\in B^*\ \exists\, b\in S^{k'}\ \exists\, j\in[s]\\ (z,b)\in B'_j \text{ and } \tau_i(a)=\tau_j(b)\end{array}\right\}.$$

We have $U_i\in\mathcal{B}(\Pi^{(k')})$ by Lemma 12. Let $H_\chi := \bigcup_{i=1}^s \tau_i(U_i)$. Then $H_\chi\in\mathcal{B}(\mathcal{S}_{\Pi,k'})$. On the other hand, note

$$H_\chi = \bigcap_{z\in B^*} W_z = \bigcap_{z\in B^*}\ker(\chi_z)\subseteq\langle B\rangle.$$

By Theorem 32, we have $H_\chi\subseteq\langle B\rangle\subseteq t(\mathbb{F}B)$. Note $t(\mathbb{F}B)\in\mathcal{B}(\mathcal{S}_{\Pi,t})$. Then $H_\chi = H_\chi\cap t(\mathbb{F}B)\in\mathcal{B}(\mathcal{S}_{\Pi,t})$ by Lemma 35 (2). As $\chi_z\in\mathcal{X}_{\Pi,k',B,\epsilon'}$ for $z\in B^*$, $\chi_x=\chi$, and $x\in B^*$, we have

$$H = \bigcap_{\chi\in\mathcal{X}_{\Pi,k',B,\epsilon'}}\ker(\chi)\subseteq H_\chi\subseteq\ker(\chi),$$

as desired.

(2): Assume to the contrary that $B\cap H\neq\emptyset$. Note $B\cap H\in\mathcal{B}(\Pi^{(1)})$ by (1) and Lemma 35 (1). As $B\in\Pi^{(1)}$, we have $B\subseteq H$ and hence $\langle B\rangle\subseteq H$. But this is impossible as $H=\bigcap_{\chi\in\mathcal{X}_{\Pi,k',B,\epsilon'}}\ker(\chi)$ is a proper subspace of $\langle B\rangle$.

(3): Every $W\in\mathcal{C}$ is of the form $H+\mathbb{F}x$ for some $x\in B$. So either $H=W$ or H is a hyperplane of W. The former case is impossible since $B\cap H=\emptyset$ by (2).

(4): By (3), we have $\dim W=\dim W'=\dim H+1$. Note $H\subseteq W\cap W'\subseteq W$. As H is a hyperplane of W, either $W\cap W'=H$ or $W\cap W'=W$. The latter case is impossible as $W\neq W'$ and $\dim W=\dim W'$.

(5): The set $T:=\{(x,y)\in B\times B: y\in H+\mathbb{F}x\}$ is in $\mathcal{B}(\Pi^{(2)})$ by (1) and Lemma 12. By Property (P2), the cardinality of $T_x:=\{y\in B:(x,y)\in T\}$ is constant when x ranges over B. But T_x is precisely $B\cap W$ where $W=H+\mathbb{F}x$. So $B\cap W$ have equal size when W ranges over $\mathcal{C}$.

(6): Let d be the codimension of H in $\langle B\rangle$. We have $\sum_{\chi\in\mathcal{X}_{\Pi,k',B,\epsilon'}}|\widehat{1_B}(\chi)|^2\leq 1$ by Parseval's identity. As $|\widehat{1_B}(\chi)|\geq\epsilon'$ for all $\chi\in\mathcal{X}_{\Pi,k',B,\epsilon}$, we have $|\mathcal{X}_{\Pi,k',B,\epsilon'}|\leq 1/\epsilon'^2$ and hence $d\leq 1/\epsilon'^2$. For every two distinct subspaces $W,W'\in\mathcal{C}$, W/H and W'/H are distinct one-dimensional subspaces of $\langle B\rangle/H$ by (3) and (4). The claim follows by noting that the number of one-dimensional subspaces of $\langle B\rangle/H$ equals $(\ell^d-1)/(\ell-1)\leq\ell^d\leq\ell^{1/\epsilon'^2}$.

(7): By (1), (3) and Lemma 36, we have $W\in\mathcal{B}(\mathcal{S}_{\Pi_x,t+1})$ for some $x\in S$. We also have $W'\in\mathcal{B}(\mathcal{S}_{\Pi_y,k''})$ for some $y\in S^{k''}$ by definition. Then $W\cap W'\in\mathcal{B}(\mathcal{S}_{\Pi_{x,y},t+1})$ by Lemma 15 and Lemma 35.

Assume $|\mu_{W\cap W'}(B) - \mu_W(B)| > \ell^d\epsilon'$. We want to prove $W \cap W' \subseteq H$, which implies $\mu_{W\cap W'}(B) = 0$ by (2). Let G_1 (resp. G_2) be the subgroup of the characters $\chi \in \widehat{\langle B\rangle}$ vanishing on $W \cap W'$ (resp. W). We have $G_2 \subseteq G_1$ and $|G_1| = |\langle B\rangle|/|W \cap W'| = \ell^d$. Note $|\mu_{W\cap W'}(B) - \mu_W(B)| = |\sum_{\chi\in G_1\setminus G_2} \widehat{1_B}(\chi)|$ (cf. Equation (10) in the proof of Lemma 39). So there exists $\chi^* \in G_1 \setminus G_2$ such that $|\widehat{1_B}(\chi^*)| \geq |G_1|^{-1}\ell^d\epsilon' = \epsilon'$. As $\chi^* \in G_1$, we have $W \cap W' \subseteq \ker(\chi^*)$. The codimension of $W \cap W'$ in $\ker(\chi^*)$ is $d-1$. So by Lemma 36 and Theorem 32, $\ker(\chi^*)$ is $((\Pi_{x,y})_{x'}, (t+1)+(d-1)t)$-constructible for some $x' \in S^{(d-1)t}$. We know $k' \geq k''+1+(d-1)t$ and $k' \geq (t+1)+(d-1)t$. It follows that $\ker(\chi^*) \in \mathcal{W}_{\Pi,k',B}$. So $\chi^* \in \mathcal{X}_{\Pi,k',B,\epsilon'}$.

Let G be the be the subgroup of the characters $\chi \in \widehat{\langle B\rangle}$ vanishing on $H \subseteq W$. As H is a hyperplane of W, G_2 is a subgroup of G of corank one. As $\chi^* \in \mathcal{X}_{\Pi,k',B,\epsilon'}$ and $H = \bigcap_{\chi\in\mathcal{X}_{\Pi,k',B,\epsilon'}} \ker(\chi)$, we have $H \subseteq \ker(\chi^*)$ and hence $\chi^* \in G$. As $\chi^* \notin G_2$, we have $G = \langle G_2, \chi^*\rangle$, which is equivalent to $H = W \cap \ker(\chi^*)$. So $W \cap W' \subseteq W \cap \ker(\chi^*) = H$, as desired. ◀

D.4 Reducing the Density of B

We adopt the following notation throughout this subsection.

▶ **Definition 42.** *For $B \in \Pi^{(2)}$ and $x \in S$, where Π is a linear m-scheme on S with $m \geq 2$, define $B_x := \{y \in S : (x,y) \in B\} \in \Pi_x^{(1)}$, called the x-*fiber *of B.*

Suppose $B \in \Pi^{(1)}$ and $B^* \in \Pi^{(2)}$ satisfy $B^* \subseteq (B\times B)\setminus\Delta_B$, where $\Delta_B := \{(x,x) : x \in B\}$. Let $B^{**} = \{(y,x) : (x,y) \in B'\}$. Then $B^{**} \in \Pi^{(2)}$, $|B^{**}| = |B^*|$, and $B^{**} \neq B^*$. So for $x \in B$, we have two distinct blocks $B_x^*, B_x^{**} \in \Pi_x^{(1)}$ of equal size contained in $B \setminus \{x\}$.

We want to prove that replacing B by B_x^* reduces the density by at least a constant factor. To achieve this, we need to restrict to a subspace in which B is pseudorandom. This leads to the following definition.

▶ **Definition 43.** *Let Π be a linear m-scheme on S. Let $B \in \Pi^{(1)}$, $k \in \mathbb{N}^+$, and $0 < \epsilon < 1$. Let $t = \lfloor \frac{3}{2\mu(B)} \rfloor + 1$, $k' = k(t+2)$ and $\epsilon' = \epsilon/\ell^k$. Suppose $m \geq 2k'$.*

1. *If $\mathcal{X}_{\Pi,k',B,\epsilon'} = \emptyset$, define $H_{\Pi,k,B,\epsilon} := \emptyset$ and $W_{\Pi,k,B,\epsilon}(x) := \langle B\rangle$ for $x \in B$.*
2. *If $\mathcal{X}_{\Pi,k',B,\epsilon'} \neq \emptyset$, define $H_{\Pi,k,B,\epsilon} := \bigcap_{\chi\in\mathcal{X}_{\Pi,k',B,\epsilon'}} \ker(\chi)$ and $W_{\Pi,k,B,\epsilon}(x) := H_{\Pi,k,B,\epsilon} + \mathbb{F}x$ for $x \in B$.*

Then B is "pseudorandom" within $W_{\Pi,k,B,\epsilon}(x)$ for each $x \in B$ in the following sense.

▶ **Lemma 44.** *Let $\Pi, m, B, k, k', \epsilon, \epsilon'$ be as in Definition 43. Suppose $m \geq 4k'$. Let $x \in B$ and $W = W_{\Pi,k,B,\epsilon}(x)$. Let $W' \in \mathcal{W}_{\Pi,k,B}$ such that $W \cap W' \not\subseteq H_{\Pi,k,B,\epsilon}$ and the codimension of $W \cap W'$ in $\langle B\rangle$ is bounded by k. Then $|\mu_{W\cap W'}(B) - \mu_W(B)| \leq \epsilon$.*

Proof. If $\mathcal{X}_{\Pi,k',B,\epsilon'} = \emptyset$, we have $W = \langle B\rangle$ by Definition 43 and hence $W \cap W' = W' \in \mathcal{W}_{\Pi,k,B}$. In this case, the lemma follows from Lemma 39. On the other hand, if $\mathcal{X}_{\Pi,k',B,\epsilon'} \neq \emptyset$, the lemma follows from Theorem 40 (7). ◀

We also need the following simple lemma.

▶ **Lemma 45.** *Let Π be a linear m-scheme and let $B \in \mathcal{B}(\Pi^{(1)})$. Suppose $|B| \geq N$ for some $N > 0$. Then there exists $B' \in \mathcal{B}(\Pi^{(1)})$ such that $B' \subseteq B$ and either of the following holds:*

1. *$N/2 \leq |B'| \leq N$.*
2. *$B' \in \Pi^{(1)}$ and $|B'| \geq N$.*

Proof. Let $T = \{B' \in \Pi^{(1)} : B' \subseteq B\}$. If there exists $B' \in T$ satisfying $|B'| \geq N/2$ then either (1) or (2) holds, depending on whether $|B'| \leq N$. So assume $|B'| < N/2$ for all $B' \in T$. Choose a minimal subset $T' \subseteq T$ such that $\sum_{B' \in T'} |B'| \geq N/2$, which is always possible as $\sum_{B' \in T} |B'| = |B| \geq N$. Let $B'' = \bigcup_{B' \in T'} B'$. Then $B'' \in \mathcal{B}(\Pi^{(1)})$, $B'' \subseteq B$, and $|B''| \geq N/2$. By the minimality of T' and the fact $|B'| < N/2$ for $B' \in T$, we have $|B''| \leq N$. So (1) holds. ◀

Next, we prove the following lemma.

▶ **Lemma 46.** *Let Π be a strongly antisymmetric linear m-scheme on S. Let $B \in \Pi^{(1)}$, $K > 1$, $t = \lfloor \frac{3K}{2\mu(B)} \rfloor + 1$, $k \in \mathbb{N}^+$, $k' = k(t+2)$, $0 < \epsilon < 1$ and $\epsilon' = \epsilon/\ell^k$. Suppose $m \geq 4k'+2$, $k \geq 2t$, and $|B| > K$. Let $x \in B$ and $W = W_{\Pi,k,B,\epsilon}(x)$, and suppose $\epsilon \leq \mu_W(B)/2$. Then one of the following holds:*

1. *There exist $y \in B$ and $B' \in \mathcal{B}(\Pi^{(1)}_{x,y})$ such that $B' \subseteq B$ and $\ell^{-(1/\epsilon'^2)}|B|/K \leq |B'| \leq |B|/K$.*
2. *There exist $B' \in \Pi^{(1)}_x$ and $y \in B'$ such that $B' \subseteq W$ and for the subspace $W' = W_{\Pi_x,k,B',\epsilon}(y)$, we have $B' \subseteq B$, $|B'| \geq |B|/K$, and $\mu_{W'}(B') \leq (\mu_W(B) + \epsilon)/2$.*
3. *There exists $B^* \in \Pi^{(2)}$ contained in $B \times B$ such that B^* and $B^{**} := \{(y,x) : (x,y) \in B^*\}$ satisfy the following conditions:*
   - **(3a)** *$B^*_x, B^{**}_x \subseteq B \cap W$, $B^*_x \neq B^{**}_x$, and $|B^*_x| = |B^{**}_x| \geq |B|/K$.*
   - **(3b)** *$W_{\Pi_x,k,B^*_x,\epsilon}(y) = \langle B^*_x \rangle$ for $y \in B^*_x$.*
   - **(3c)** *$W_{\Pi_x,k,B^{**}_x,\epsilon}(y) = \langle B^{**}_x \rangle$ for $y \in B^{**}_x$, and $\dim\langle B^{**}_x \rangle = \dim\langle B^*_x \rangle$.*
   - **(3d)** *$B \cap \langle B^*_x \rangle \cap \langle B^{**}_x \rangle = \emptyset$.*
   - **(3e)** *$x \in \langle B^*_x \rangle$.*
   - **(3f)** *$|(B \cap \langle B^*_x \rangle) \setminus B^*_x|, |(B \cap \langle B^{**}_x \rangle) \setminus B^{**}_x| < \ell^{-(1/\epsilon'^2)}|B|/K$.*

Case (1) basically implies Lemma 21 (for large enough K). So we are done in this case. We give some intutions for Case (2) and (3). For simplicity, assume $W = \langle B \rangle$.

As mentioned above, the set $B \setminus \{x\}$ contains two distinct blocks $B^*_x, B^{**}_x \in \Pi^{(1)}_x$ of equal size as subsets. Assume B^*_x and B^{**}_x are dense enough in $\langle B \rangle$. Let $H = \langle B^*_x \rangle \cap \langle B^{**}_x \rangle$. Then it is not hard to show that either $H \in \{\langle B^*_x \rangle, \langle B^{**}_x \rangle\}$ or $B^*_x \cap H = B^{**}_x \cap H = \emptyset$. Otherwise, we could intersect either B^*_x or B^{**}_x with H and obtain a nonempty proper subset of B^*_x or B^{**}_x that is in $\mathcal{B}(\Pi^{(1)}_x)$, contradicting $B^*_x, B^{**}_x \in \Pi^{(1)}_x$.

Assume $H = \langle B^*_x \rangle = \langle B^{**}_x \rangle$. As B is pseudorandom within W, we have $\mu_H(B) \approx \mu_W(B)$. As $B^*_x, B^{**}_x \subseteq B$ and $B^*_x \cap B^{**}_x = \emptyset$, we have

$$\min\{\mu(B^*_x), \mu(B^{**}_x)\} = \min\{\mu_H(B^*_x), \mu_H(B^{**}_x)\} \leq \mu_H(B)/2 \approx \mu_W(B)/2.$$

A similar argument shows that this holds more generally when $H \in \{\langle B^*_x \rangle, \langle B^{**}_x \rangle\}$. Moreover, in order to apply Lemma 46 repeatedly, we will actually find some $B' \in \Pi^{(1)}_x$ and a subspace W' such that $\mu_{W'}(B') \lessapprox \mu_W(B)/2$ and B' is pseudorandom within W'. This is captured by Case (2).

Unfortunately, this argument does not seem to work in the case $B^*_x \cap H = B^{**}_x \cap H = \emptyset$, and we do not know how to rule out this case. This exceptional case is described by Case (3) above and will be addressed later via a careful analysis (see Lemma 49 below).

Proof of Lemma 46. As the proof is long and technical, we divide it into several steps.

Step 1: Finding $B' \in \Pi^{(1)}_x$ such that $B' \subseteq B \cap W$ and $|B'| \geq |B|/K$.

If $\mathcal{X}_{\Pi,k',B,\epsilon'} = \emptyset$, we have $W = \langle B \rangle = t(\mathbb{F}B) \in \mathcal{B}(\mathcal{S}_{\Pi,t})$ by Theorem 32. And if $\mathcal{X}_{\Pi,k',B,\epsilon'} \neq \emptyset$, we have $H_{\Pi,k,B,\epsilon} \in \mathcal{B}(\mathcal{S}_{\Pi,t})$ by Theorem 40 (1) and hence $W = H_{\Pi,k,B,\epsilon} + \mathbb{F}x \in \mathcal{B}(\mathcal{S}_{\Pi_x,t+1})$. In either case, we have $W \in \mathcal{B}(\mathcal{S}_{\Pi_x,t+1})$. So $B \cap W \in \mathcal{B}(\Pi^{(1)}_x)$ by Lemma 35 (1).

Also note $|B \cap W| \geq \ell^{-1/\epsilon'^2}|B|$. This is trivial if $\mathcal{X}_{\Pi,k',B,\epsilon'} = \emptyset$, in which case $W = \langle B \rangle$. Otherwise it follows from Theorem 40 (4), (5) and (6).

If $|B \cap W| \leq |B|/K$ then Case (1) holds. So assume $|B \cap W| \geq |B|/K$. Applying Lemma 45 to Π_x, $B \cap W \in \mathcal{B}(\Pi_x^{(1)})$ and $N = |B|/K$, we see that there exists $B' \in \mathcal{B}(\Pi_x^{(1)})$ such that $B' \subseteq B \cap W$ and either of the following holds:

(a) $|B|/(2K) \leq |B'| \leq |B|/K$.

(b) $B' \in \Pi_x^{(1)}$ and $|B'| \geq |B|/K$.

In the former case, Case (1) holds and we are done. So assume $B' \in \Pi_x^{(1)}$ and $|B'| \geq |B|/K$.

In the following, we choose B' such that $\dim\langle B' \rangle$ is minimized subject to the conditions $B' \in \Pi_x^{(1)}$, $B' \subseteq B \cap W$ and $|B'| \geq |B|/K$.

Step 2: Proving (3a).

Choose B^* to be the block in $\Pi^{(2)}$ satisfying $B' = \{y \in S : (x, y) \in B^*\}$. Then $B_x^* = B' \subseteq B \cap W$. Let $B^{**} = \{(y, x) : (x, y) \in B^*\} \in \Pi^{(2)}$ as in (3). As $x \in B$ and $B' \subseteq B$, we have $B^* \cap (B \times B) \neq \emptyset$ and hence $B^*, B^{**} \subseteq B \times B$. So $B_x^{**} \subseteq B$. By Property (P2), we have $|B_x^*| = |B^*|/|B|$ and $|B_x^{**}| = |B^{**}|/|B|$. As $|B^*| = |B^{**}|$, we have $|B_x^*| = |B_x^{**}| = |B'| \geq |B|/K > 1$. As $|B_x^*| > 1$, there exists $y \in B_x^*$ different from x. Then $(x, y) \in B^*$ and $(y, x) \in B^{**}$. The map $(a, b) \mapsto (b, a)$ sends B^* to B^{**} and does not fix (x, y). By strong antisymmetry of Π, $B^* \neq B^{**}$. So $B_x^* \neq B_x^{**}$.

It remains to prove $B_x^{**} \subseteq W$. Let $y \in B_x^*$ and $z \in B_x^{**}$. Then $y \in B \cap W$ and $(y, x), (x, z) \in B^{**}$. We want to prove $z \in W$. As $x \in W$, we have $y \in H_{\Pi,k,B,\epsilon} + \mathbb{F}x$ by Theorem 40 (2) and (3). By Theorem 40 (1), $H_{\Pi,k,B,\epsilon} \in \mathcal{B}(\mathcal{S}_{\Pi,t})$. So there exist $B_1, \ldots, B_s \in \Pi^{(t)}$ and $\tau_1, \ldots, \tau_s \in \mathcal{M}_{t,1}$ such that $H_{\Pi,k,B,\epsilon} = \bigcup_{i=1}^s \tau_i(B_i)$. Then (y, x) satisfies the relation $y - cx \in \bigcup_{i=1}^s \tau_i(B_i)$ for some $c \in \mathbb{F}^\times$. As (y, x) and (x, z) are in the same block of $\Pi^{(2)}$, we have $x - cz \in \bigcup_{i=1}^s \tau_i(B_i) = H_{\Pi,k,B,\epsilon}$. So $z \in c^{-1}x + H_{\Pi,k,B,\epsilon} = W$, as desired.

Step 3: Proving (3b).

For $y \in B_x^*$, the definition only guarantees $W_{\Pi_x,k,B_x^*,\epsilon}(y)$ to be a subspace of $\langle B_x^* \rangle$. However, as $B_x^* = B'$ is chosen such that $\dim\langle B' \rangle$ is minimized, we actually have $W_{\Pi_x,k,B_x^*,\epsilon}(y) = \langle B_x^* \rangle$. The reason is that if $W_{\Pi_x,k,B_x^*,\epsilon}(y) \subsetneq \langle B_x^* \rangle$, we could use $H_{\Pi_x,k,B_x^*,\epsilon}$ to find another block $B'' \in \Pi_x^{(1)}$ satisfying the same conditions that are satisfied by B' and additionally $\dim\langle B'' \rangle < \dim\langle B' \rangle$ holds. But this contradicts the minimality of $\dim\langle B' \rangle$.

To formalize this argument, we first prove the following claim.

▷ Claim 47. Suppose W' is a (Π_x, k)-constructible subspace of W such that $B \cap W' \neq \emptyset$ and the codimension of W' in $\langle B \rangle$ is at most k. Then either Case (1) of Lemma 46 holds or there exists $B'' \in \Pi_x^{(1)}$ satisfying $B'' \subseteq B \cap W'$ and $|B''| \geq |B|/K$. Moreover, in the latter case, $\dim\langle B_x^* \rangle \leq \dim\langle B'' \rangle \leq \dim W'$.

Proof of Claim 47. As W' is a (Π_x, k)-constructible and its codimension in $\langle B \rangle$ is at most k, we have $W' \in \mathcal{W}_{\Pi,k,B}$ by definition. As $B \cap W' \neq \emptyset$, we have $W' \not\subseteq H_{\Pi,k,B,\epsilon}$ by Theorem 40 (2). By Lemma 44,

$$\mu_{W'}(B) = \mu_{W \cap W'}(B) \geq \mu_W(B) - \epsilon \geq \mu_W(B)/2.$$

Therefore

$$\begin{aligned} |B \cap W'| &\geq \mu_W(B)/2 \cdot |W'| \geq \mu_W(B)|W|/(2\ell^k) = |B \cap W|/(2\ell^k) \\ &\geq |B|/(2K\ell^k) \geq \ell^{-(1/\epsilon'^2)}|B|/K. \end{aligned}$$

As W' is a (Π_x, k)-constructible, we have $B \cap W' \in \mathcal{B}(\Pi_x^{(1)})$ by Lemma 35 (1). If $|B \cap W'| \leq |B|/K$ then Case (1) holds. So assume $|B \cap W'| \geq |B|/K$. Applying Lemma 45 to Π_x, $B \cap W'$

and $N = |B|/K$, we see that there exists $B'' \in \mathcal{B}(\Pi_x^{(1)})$ such that $B'' \subseteq B \cap W' \subseteq B \cap W$ and either of the following holds:

(a) $|B|/(2K) \le |B''| \le |B|/K$.

(b) $B'' \in \Pi_x^{(1)}$ and $|B''| \ge |B|/K$.

In the former case, Case (1) holds. So assume $B'' \in \Pi_x^{(1)}$ and $|B''| \ge |B|/K$. We then have $\dim\langle B_x^*\rangle = \dim\langle B'\rangle \le \dim\langle B''\rangle \le \dim W'$ by the minimality of $\dim\langle B'\rangle$ subject to the conditions $B' \in \Pi_x^{(1)}$, $B' \subseteq B \cap W$ and $|B'| \ge |B|/K$. ◁

Now we prove (3b). If $\mathcal{X}_{\Pi_x,k',B_x^*,\epsilon'} = \emptyset$, then (3b) holds by Definition 43. So assume $\mathcal{X}_{\Pi_x,k',B_x^*,\epsilon'} \neq \emptyset$.

We want to prove $W_{\Pi_x,k,B_x^*,\epsilon}(y) = \langle B_x^*\rangle$ for $y \in \langle B_x^*\rangle$. Let $H = H_{\Pi_x,k,B_x^*,\epsilon} \subseteq \langle B_x^*\rangle$. As H is a hyperplane of $W_{\Pi_x,k,B_x^*,\epsilon}(y)$ for $y \in \langle B_x^*\rangle$, it suffices to prove $\dim H \ge \dim\langle B_x^*\rangle - 1$.

Let $W' = H + \mathbb{F}x \subseteq W$. We check that W' satisfies the conditions in Claim 47:

- As $x \in B \cap W'$, we have $B \cap W' \neq \emptyset$.
- By Theorem 40 (1), $H \in \mathcal{B}(\mathcal{S}_{\Pi_x,t})$. As $\{x\} \in \Pi_x^{(1)}$, we have $W' = H + \mathbb{F}x \in \mathcal{B}(\mathcal{S}_{\Pi_x,t+1}) \subseteq \mathcal{B}(\mathcal{S}_{\Pi_x,k})$. So W' is (Π_x, k)-constructible.
- Let $y \in B_x^*$ and $W'' = W_{\Pi_x,k,B_x^*,\epsilon}(y) = H + \mathbb{F}y$. Then $W'' \in \mathcal{B}(\mathcal{S}_{\Pi_{x,y},t+1})$ and hence $B_x^* \cap W'' \in \Pi_{x,y}^{(1)}$ by Lemma 35 (1). By Theorem 40 (4), (5) and (6), we have

  $$|B_x^* \cap W''| \ge \ell^{-1/\epsilon'^2}|B_x^*| \ge \ell^{-1/\epsilon'^2}|B|/K.$$

  If $|B_x^* \cap W''| \le |B|/K$ then Case (1) holds. So assume $|B_x^* \cap W''| \ge |B|/K$. Then the codimension of W'' in $\langle B\rangle$ is at most $\log_\ell(K/\mu(B)) \le t \le k-1$. As $\dim W' = \dim(H + \mathbb{F}x) \ge \dim(H + \mathbb{F}y) - 1 = \dim W'' - 1$, the codimension of W' in $\langle B\rangle$ is at most k.

By Claim 47, either Case (1) holds or $\dim W' \ge \dim\langle B_x^*\rangle$. Assume the latter case occurs. As $W' = H + \mathbb{F}x$, we have $\dim H \ge \dim\langle B_x^*\rangle - 1$, as desired.

Step 4: Proving (3c).

Let $y \in B_x^{**}$ and $W' = W_{\Pi_x,k,B_x^{**},\epsilon}(y) = H' + \mathbb{F}y$. We want to prove $\dim\langle B_x^*\rangle = \dim\langle B_x^{**}\rangle$ and $W' = \langle B_x^{**}\rangle$ (if neither Case (1) nor (2) holds).

We first show that either Case (2) holds or $\dim W' \le \dim\langle B_x^*\rangle$. By Lemma 44 and (3b), we have

$$\mu(B_x^*) \le \mu_{\langle B_x^*\rangle}(B) = \mu_{W\cap\langle B_x^*\rangle}(B) \le \mu_W(B) + \epsilon. \tag{11}$$

Note $|B_x^{**}| = |B_x^*|$. If $\dim W' > \dim\langle B_x^*\rangle$, then

$$\mu_{W'}(B_x^{**}) \le \frac{|B_x^*|}{|W'|} \le \frac{|B_x^*|}{2|\langle B_x^*\rangle|} = \mu(B_x^*)/2 \overset{(11)}{\le} (\mu_W(B) + \epsilon)/2$$

and hence Case (2) holds. So assume $\dim W' \le \dim\langle B_x^*\rangle$.

Consider the case $\mathcal{X}_{\Pi_x,k',B_x^{**},\epsilon'} = \emptyset$. Then $W' = \langle B_x^{**}\rangle$ by Definition 43. So $\dim\langle B_x^{**}\rangle \le \dim\langle B_x^*\rangle$. Exchanging B_x^* and B_x^{**} in the above proof shows $\dim\langle B_x^*\rangle \le \dim\langle B_x^{**}\rangle$ (or Case (2) holds). So $\dim\langle B_x^*\rangle = \dim\langle B_x^{**}\rangle$ and (3c) holds.

So assume $\mathcal{X}_{\Pi_x,k',B_x^{**},\epsilon'} \neq \emptyset$. Let $H' = H_{\Pi_x,k,B_x^{**},\epsilon}$. In Step 3, we have shown that $H_{\Pi_x,k,B_x^*,\epsilon} + \mathbb{F}x$ satisfies the conditions in Claim 47. The same proof with B_x^* replaced by B_x^{**} also shows $W' = H' + \mathbb{F}x$ satisfies the conditions in Claim 47. Applying Claim 47 to W', we see either Case (1) holds or $\dim W' \ge \dim\langle B_x^*\rangle$. Assume the latter. Then $\dim W' = \dim\langle B_x^*\rangle$ as we already know $\dim W' \le \dim\langle B_x^*\rangle$.

It remains to prove $W' = \langle B_x^{**} \rangle$ (or Case (1) or (2) holds). Assume W' is a proper subspace of $\langle B_x^{**} \rangle$. Then $|B_x^{**} \cap W'| \leq |B_x^{**}|/2$ by Theorem 40 (4) and (5). Therefore

$$\mu_{W'}(B_x^{**}) \leq \frac{|B_x^{**}|}{2|W'|} = \frac{|B_x^{*}|}{2|\langle B_x^{*} \rangle|} = \mu(B_x^*)/2 \overset{(11)}{\leq} (\mu_W(B) + \epsilon)/2$$

and hence Case (2) holds.

Step 5: Proving (3d).

Assume neither Case (1) nor (2) holds. Also assume $B \cap \langle B_x^* \rangle \cap \langle B_x^{**} \rangle \neq \emptyset$. We will derive a contradiction. The intuition is that since $B \cap \langle B_x^* \rangle \cap \langle B_x^{**} \rangle \neq \emptyset$, we could find another block $B'' \subseteq B \cap \langle B_x^* \rangle \cap \langle B_x^{**} \rangle$ and use it to contradict the minimality of $\dim\langle B' \rangle$.

Let $W' = \langle B_x^* \rangle \cap \langle B_x^{**} \rangle \subseteq W$. We check that W' satisfies the conditions in Claim 47:

- By assumption, we have $B \cap W' = B \cap \langle B_x^* \rangle \cap \langle B_x^{**} \rangle \neq \emptyset$.
- As $|B_x^*| = |B_x^{**}| \geq |B|/K$, both $\mu(B_x^*)$ and $\mu(B_x^{**})$ are at least $\mu_{\langle B \rangle}(B_x^*) = \mu_{\langle B \rangle}(B_x^{**}) \geq \mu(B)/K$. By Theorem 32, $\langle B_x^* \rangle$ and $\langle B_x^{**} \rangle$ are (Π_x, t)-constructible and hence (Π_x, k)-constructible. By Lemma 35 (2), $W' = \langle B_x^* \rangle \cap \langle B_x^{**} \rangle$ is also (Π_x, k)-constructible.
- As $\mu_{\langle B \rangle}(B_x^*) = \mu_{\langle B \rangle}(B_x^{**}) \geq \mu(B)/K$, both $\langle B_x^* \rangle$ and $\langle B_x^{**} \rangle$ have codimension at most $\log_\ell(K/\mu(B)) \leq t$ in $\langle B \rangle$. So $W' = \langle B_x^* \rangle \cap \langle B_x^{**} \rangle$ has codimension at most $2t \leq k$ in $\langle B \rangle$.

By Claim 47, we have $\dim W' \geq \dim\langle B_x^* \rangle$. Then $W' = \langle B_x^* \rangle = \langle B_x^{**} \rangle$ by (3c). As W' is (Π_x, k)-constructible and its codimension in $\langle B \rangle$ is at most k, we have $W' \in \mathcal{W}_{\Pi,k,B}$ by definition. As $B_x^*, B_x^{**} \subseteq B$, $B_x^* \cap B_x^{**} = \emptyset$, and $|B_x^*| = |B_x^{**}|$, we have

$$\mu_{W'}(B_x^*) \leq \mu_{W'}(B)/2 = \mu_{W \cap W'}(B)/2 \leq (\mu_W(B) + \epsilon)/2.$$

where the last inequality holds by Lemma 44. By (3b), $W' = W_{\Pi_x,k,B_x^*,\epsilon}(y)$ for $y \in B_x^*$. So Case (2) holds, contradicting our assumption.

Step 6: Addressing the case $\mathcal{X}_{\Pi,k',B,\epsilon'} = \emptyset$.

Let $W' = \langle B_x^* \rangle \cap \langle B_x^{**} \rangle$ as in Step 5. Suppose $\mathcal{X}_{\Pi,k',B,\epsilon'} = \emptyset$. Then $H_{\Pi,k,B,\epsilon} = \emptyset$ and hence $W' \not\subseteq H_{\Pi,k,B,\epsilon}$. By Lemma 44, we have

$$\mu_{W'}(B) = \mu_{W \cap W'}(B) \geq \mu_W(B) - \epsilon > 0.$$

So $B \cap \langle B_x^* \rangle \cap \langle B_x^{**} \rangle \neq \emptyset$. By Step 5, either Case (1) or (2) holds.

From now on, we assume $\mathcal{X}_{\Pi,k',B,\epsilon'} \neq \emptyset$, so that $H_{\Pi,k,B,\epsilon}$ is a hyperplane of W.

Step 7: Proving (3e).

We want to prove $x \in \langle B_x^* \rangle$. While we do not know if this holds in general, we will show that it can be achieved by replacing $B_x^* = B'$ with another block and $\dim\langle B' \rangle$ remains minimized.

Let $H = H_{\Pi,k,B,\epsilon}$, which is a hyperplane of W by Step 6. Let $W' = (\langle B_x^* \rangle \cap H) + \mathbb{F}x \subseteq W$. We check that W' satisfies the conditions in Claim 47:

- As $x \in B \cap W'$, we have $B \cap W' \neq \emptyset$.
- By Theorem 40 (1), $H \in \mathcal{B}(\mathcal{S}_{\Pi,t}) \subseteq \mathcal{B}(\mathcal{S}_{\Pi_x,t})$. We also know $\langle B_x^* \rangle \in \mathcal{B}(\mathcal{S}_{\Pi_x,t})$ (see Step 5). So $\langle B_x^* \rangle \cap H \in \mathcal{B}(\mathcal{S}_{\Pi_x,t})$ by Lemma 35 (2). As $\{x\} \in \Pi_x^{(1)}$, we have $W' = (\langle B_x^* \rangle \cap H) + \mathbb{F}x \in \mathcal{B}(\mathcal{S}_{\Pi_x,t+1}) \subseteq \mathcal{B}(\mathcal{S}_{\Pi_x,k})$, i.e., W' is (Π_x, k)-constructible.
- We already know the codimension of $\langle B_x^* \rangle$ in $\langle B \rangle$ is at most k (see Step 5). As $\dim W' = \dim(\langle B_x^* \rangle \cap H) + 1 = \dim\langle B_x^* \rangle$, the codimension of W' in $\langle B \rangle$ is at most k.

By Claim 47, either (1) holds or there exists $B'' \in \Pi_x^{(1)}$ satisfying $B'' \subseteq B \cap W' \subseteq B \cap W$, $|B''| \geq |B|/K$, and $\dim\langle B_x^* \rangle = \dim\langle B' \rangle \leq \dim\langle B'' \rangle \leq \dim W'$. Assume the latter case occurs. We know $\dim W' = \dim\langle B_x^* \rangle$. So $\dim\langle B'' \rangle = \dim\langle B' \rangle$ and $\langle B'' \rangle = W' \ni x$. Replacing B' by B'' preserves the conditions $B' \in \Pi_x^{(1)}$, $B' \subseteq B \cap W$ and $|B'| \geq |B|/K$, and $\dim\langle B' \rangle$

remains minimized subject to these conditions. So, by replacing B' with B'', we may assume $x \in \langle B' \rangle = \langle B'^*_x \rangle$, and all the results proved above still hold.

Step 8: Proving (3f).

We prove that $|(B \cap \langle B^{**}_x \rangle) \setminus B^{**}_x| < \ell^{-(1/\epsilon'^2)}|B|/K$ (or either Case (1) or (2) holds). The proof for the claim $|(B \cap \langle B^*_x \rangle) \setminus B^*_x| < \ell^{-(1/\epsilon'^2)}|B|/K$ is the same.

Let $T = (B \cap \langle B^{**}_x \rangle) \setminus B^{**}_x$. We have $T \in \mathcal{B}(\Pi^{(1)}_x)$ by Lemma 35 (1). If $\ell^{-(1/\epsilon'^2)}|B|/K \le |T| \le |B|/K$ then (1) holds.

Now assume $|T| \ge |B|/K$. Applying Lemma 45 to Π_x, T and $N = |B|/K$, we see that there exists $T' \in \mathcal{B}(\Pi^{(1)}_x)$ such that $T' \subseteq T \subseteq \langle B^{**}_x \rangle$ and either of the following holds:

(a) $|B|/(2K) \le |T'| \le |B|/K$.

(b) $T' \in \Pi^{(1)}_x$ and $|T'| \ge |B|/K$.

In the former case, Case (1) holds and we are done. So assume $T' \in \Pi^{(1)}_x$ and $|T'| \ge |B|/K$.

Let $H = H_{\Pi_x,k,T',\epsilon}$. Define a subspace W' of W as follows: If $\mathcal{X}_{\Pi_x,k',T',\epsilon'} = \emptyset$, let $W' = \langle T' \rangle$. Otherwise let $W' = H + \mathbb{F}x$. Note that in either case, we have $\dim W' = \dim W_{\Pi_x,k,T',\epsilon}(y)$ for $y \in T'$. Using the fact $|T'| \ge |B|/K$, it can be shown that either Case (1) holds or W' satisfies the conditions in Claim 47.[2] Assume the latter case occurs.

By Claim 47, we have $\dim W' \ge \dim\langle B^*_x \rangle = \dim\langle B^{**}_x \rangle$. Therefore, $\dim W_{\Pi_x,k,T',\epsilon}(y) \ge \dim\langle B^{**}_x \rangle$ for $y \in T'$. As $T' \subseteq \langle B^{**}_x \rangle$, we have $W_{\Pi_x,k,T',\epsilon}(y) = \langle B^{**}_x \rangle$ for $y \in T'$.

As $T', B^{**}_x \subseteq B \cap \langle B^{**}_x \rangle$ and $T' \cap B^{**}_x = \emptyset$, we have

$$\min\{\mu_{\langle B^{**}_x \rangle}(T'), \mu(B^{**}_x)\} \le \mu_{\langle B^{**}_x \rangle}(B)/2 = \mu_{W \cap \langle B^{**}_x \rangle}(B)/2 \le (\mu_W(B) + \epsilon)/2$$

where the last inequality holds by Lemma 44 and (3c). So Case (2) holds.

Therefore, we may assume $|T| < \ell^{-(1/\epsilon'^2)}|B|/K$, since otherwise Case (1) or (2) holds. ◀

To address Case (3) of Lemma 46, we need the following lemma.

▶ **Lemma 48.** *Let Π be a linear m-scheme on S, where $m \ge 2$. Let $B \in \Pi^{(1)}$ and $B', B'' \in \Pi^{(2)}$ such that $B', B'' \subseteq B \times B$. Let $x \in B$, $\mu = |B'_x|/|\langle B \rangle|$ and $t = \lfloor \frac{3}{2\mu} \rfloor + 1$. Suppose $m \ge t + 1$. For $y \in B$, we have (1) $|B''_y| = |B''_x|$, (2) either $B''_y \subseteq \langle B'_y \rangle$ or $B''_y \cap \langle B'_y \rangle = \emptyset$, and (3) $B''_y \subseteq \langle B'_y \rangle$ iff $B''_x \subseteq \langle B'_x \rangle$.*

Proof. The first claim holds by Property (P2) of Π. Also note $|B'_y| = |B'_x|$ and hence $\mu(B'_y) \ge \mu$ for $y \in B$ by Property (P2) of Π.

Consider $y \in B$. By Theorem 32 and the fact $\mu(B'_y) \ge \mu$, we have $\langle B'_y \rangle \in \mathcal{B}(\mathcal{S}_{\Pi_y,t})$. By Lemma 35 (1), we have $B''_y \cap \langle B'_y \rangle \in \mathcal{B}(\Pi^{(1)}_y)$. As $B''_y \in \Pi^{(1)}_y$, $B''_y \cap \langle B'_y \rangle$ equals either B''_y or the empty set. This proves (2).

Let T be the set of $y \in B$ satisfying $B''_y \subseteq \langle B'_y \rangle$, or equivalently, $B''_y \cap \langle B'_y \rangle \ne \emptyset$. Then $T = \bigcup_{\tau \in \mathcal{M}_{t,1}} T_\tau$, where

$$T_\tau = \left\{ y \in B : \begin{array}{l} \exists\, z = (z_1, \ldots, z_t) \in B^t \text{ such that} \\ (y, z_1) \in B', \ldots, (y, z_t) \in B', (y, \tau(z)) \in B'' \end{array} \right\}.$$

So $T \in \mathcal{B}(\Pi^{(1)})$ by Lemma 12. As $B \in \Pi^{(1)}$, either $T = B$ or $T = \emptyset$. This proves (3). ◀

Next, we prove that Case (3) of Lemma 46 actually implies Case (1):

---

[2] We omit the proof. If $\mathcal{X}_{\Pi_x,k',T',\epsilon'} = \emptyset$, we have $W' = \langle T' \rangle$ and the proof is similar to that in Step 5. Otherwise, we have $W' = H + \mathbb{F}x$ and the proof is similar to that in Step 3.

▶ **Lemma 49.** *Under the notations of Lemma 46, further assume $k \geq (t+1)\log_\ell(K/\mu(B))$. If Case (3) of Lemma 46 holds, then Case (1) also holds.*

Proof. Assume Case (3) of Lemma 46 holds. By Theorem 32 and (3a), $\langle B_x^* \rangle = t(\mathbb{F}B_x^*)$. As $x \in \langle B_x^* \rangle$ by (3e), we may choose $x_1, \ldots, x_t \in B_x^*$ such that x is in the linear span of $x_1, \ldots, x_t$ over $\mathbb{F}$. As $|B_x^*| \geq |B|/K > 1$ and $\{x\}, B_x^* \in \Pi_x^{(1)}$, we have $x \notin B_x^*$ and hence $x \notin \{x_1, \ldots, x_t\}$.

As $x_1, \ldots, x_t \in B_x^*$, we have $x \in B_{x_i}^{**}$ for $i \in [t]$. Define $L := \langle B_x^* \rangle \cap \bigcap_{i=1}^t \langle B_{x_i}^{**} \rangle \subseteq W$. Then $x \in L$. For $i \in [t]$, define $T_i := (B \cap \langle B_{x_i}^{**} \rangle) \setminus B_{x_i}^{**}$. By (3f) and Lemma 48, we have $|T_i| = |(B \cap \langle B_x^{**} \rangle) \setminus B_x^{**}| < N$ for $i \in [t]$, where $N := \ell^{-(1/\epsilon'^2)}|B|/K$.

Let U be the union of all the blocks $B' \in \Pi_x^{(1)}$ satisfying $B' \subseteq B$ and $|B'| \leq N$. Then $U \in \mathcal{B}(\Pi_x^{(1)})$. If $|U| \geq 2N$, then as U is a union of blocks of cardinality at most N, there exists a subset $U' \subseteq U$ in $\mathcal{B}(\Pi_x^{(1)})$ such that $N \leq |U'| \leq 2N \leq |B|/K$. Then Case (1) of Lemma 46 holds. So we may assume $|U| \leq 2N$.

Note $\langle B_x^* \rangle \in \mathcal{B}(\mathcal{S}_{\Pi_x,t})$ and $\langle B_{x_i}^{**} \rangle \in \mathcal{B}(\mathcal{S}_{\Pi_{x_i},t})$ for $i \in [t]$. By Lemma 35 (2), we have $L \in \mathcal{B}(\mathcal{S}_{\Pi_{x,x_1,\ldots,x_t},t})$. As $|B_x^*| \geq |B|/K$ and $|B_{x_i}^{**}| = |B_x^{**}| \geq |B|/K$ for $i \in [t]$, the codimension of L in $\langle B \rangle$ is at most $(t+1)\log_\ell(K/\mu(B)) \leq k$. By definition, we have $L \in \mathcal{W}_{\Pi,k,B}$.

As $x \in L$, we have $L \not\subseteq H_{\Pi,k,B,\epsilon}$. So $|\mu_L(B) - \mu_W(B)| \leq \epsilon$ by Lemma 44. Therefore

$$\begin{aligned} |B \cap L| &\geq (\mu_W(B) - \epsilon) \cdot |L| \geq \mu_W(B)/2 \cdot |L| \geq \mu_W(B)/2 \cdot \ell^{-k} \cdot |W| \\ &= |B \cap W|/(2\ell^k) \geq |B|/(2\ell^k K) \geq (t+2)N > |U| + \sum_{i=1}^t |T_i|. \end{aligned}$$

Therefore, there exists $y \in B \cap L$ such that $y \notin U$ and $y \notin T_i$ for $i \in [t]$. Fix such y.

For $i \in [t]$, we have $y \in (B \cap \langle B_{x_i}^{**} \rangle) \setminus T_i = B_{x_i}^{**}$, i.e., $(x_i, y) \in B^{**}$, or equivalently, $(y, x_i) \in B^*$. So $x_i \in B_y^* \subseteq \langle B_y^* \rangle$ for $i \in [t]$. As x is in the linear span of $x_1, \ldots, x_t$, we have $x \in \langle B_y^* \rangle$.

Let B' (resp. B'') be the block in $\Pi^{(2)}$ containing (x, y) (resp. (y, x)). Then $|B'| = |B''|$. Note that B'_x is the block in $\Pi_x^{(1)}$ containing y. As $y \notin U$, we have $|B'_x| > N$. Then $|B''_y| > N$ since $|B''_y| = |B''|/|B| = |B'|/|B| = |B'_x|$ by Property (P2) of Π.

Note that B''_y is the block in $\Pi_y^{(1)}$ containing x. As $x \in \langle B_y^* \rangle$, we have $B''_y \subseteq B \cap \langle B_y^* \rangle$ by Lemma 48. By (3f) and Lemma 48, we have $|(B \cap \langle B_y^* \rangle) \setminus B_y^*| = |(B \cap \langle B_x^* \rangle) \setminus B_x^*| < N$. As $|B''_y| > N$, we must have $B''_y = B_y^*$. So $x \in B_y^*$, or equivalently, $y \in B_x^{**}$.

As $y \in L \subseteq \langle B_x^* \rangle$, we have $y \in \langle B_x^* \rangle \cap \langle B_x^{**} \rangle$. So $B \cap \langle B_x^* \rangle \cap \langle B_x^{**} \rangle \neq \emptyset$, contradicting (3d). ◀

Combining Lemma 46 with Lemma 49, we obtain the following lemma, which will be used to prove Lemma 21 in the next Subsection.

▶ **Lemma 50.** *Let Π be a strongly antisymmetric linear m-scheme on S. Let $B \in \Pi^{(1)}$, $K > 1$, $t = \lfloor \frac{3K}{2\mu(B)} \rfloor + 1$, $k \in \mathbb{N}^+$, $k' = k(t+2)$, $0 < \epsilon < 1$ and $\epsilon' = \epsilon/\ell^k$. Suppose $m \geq 4k'+2$, $k \geq 2t$, $k \geq (t+1)\log_\ell(K/\mu(B))$, and $|B| > K$. Let $x \in B$ and $W = W_{\Pi,k,B,\epsilon}(x)$, and suppose $\epsilon \leq \mu_W(B)/2$. Then one of the following holds:*

1. *There exist $y \in B$ and $B' \in \mathcal{B}(\Pi_{x,y}^{(1)})$ such that $B' \subseteq B$ and $\ell^{-(1/\epsilon'^2)}|B|/K \leq |B'| \leq |B|/K$.*
2. *There exist $B' \in \Pi_x^{(1)}$ and $y \in B'$ such that $B' \subseteq W$ and for the subspace $W' = W_{\Pi_x,k,B',\epsilon}(y)$, we have $B' \subseteq B$, $|B'| \geq |B|/K$, and $\mu_{W'}(B') \leq (\mu_W(B) + \epsilon)/2$.*

D.5 Finishing the Proof of Lemma 21

Lemma 21 can be easily derived from the following lemma.

▶ **Lemma 51.** *Let Π be a strongly antisymmetric linear m-scheme on S. Let $B \in \Pi^{(1)}$ and $K \geq 4$. Let $k = 6K^4$, $r = \lceil \log K / \log\log K \rceil + 1$, $\epsilon = (2/3)^{r-1}/3$ and $\epsilon' = \epsilon/\ell^k$. Suppose $|B| \geq |\langle B \rangle|/K$, $|B| > K^2$ and $m \geq 120K^7 + 3r$. Then there exist $x_1, \ldots, x_{3r+1} \in B$ and $B' \in \mathcal{B}(\Pi^{(1)}_{x_1,\ldots,x_{3r+1}})$ such that $B' \subseteq B$ and*

$$\ell^{-(1/\epsilon'^2)}|B|/K^3 \leq |B'| \leq \max\{K^{-1}, (2\gamma)^r\} \cdot |B|.$$

where $\gamma := 4\left((r-1)/\log \ell\right)^{-1/20}$.

We prove Lemma 51 in two steps. First, we repeatedly apply Lemma 50 r times for some $r = \omega(1)$. If Case (1) of Lemma 50 ever occurs then we are done. So assume Case (2) holds each time. This enables us to find a block $B' \in \Pi^{(1)}_{x_1,\ldots,x_r}$ contained in B and a subspace W such that $\mu_W(B') \leq \exp(-r)$ and B' is pseudorandom within W.

Let $B'' = B' \cap W$. The condition $\mu_W(B') \leq \exp(-r)$ implies $|B'' + B''| \gg |B''|$ by the Freiman–Ruzsa Theorem. In the second step of the proof, we use this condition to reduce the cardinality of B'' r times such that each time the cardinality is reduced by a superconstant factor. The ideas here are similar to those in the proof of Lemma 19. However, Lemma 19 itself is not sufficient here[3] and we need to augment it with the Balog-Szemerédi-Gowers Theorem for linear m-schemes (Theorem 33).

Proof of Lemma 51. As mentioned above, the proof consists of two steps:

Step 1: Finding a sparse block.

We claim that for $0 \leq i \leq r$, there exist $x_1, \ldots, x_i \in B$ and $T(i) \subseteq B$ such that either of the following holds:

(a) $T(i) \in \mathcal{B}(\Pi^{(1)}_{x_1,\ldots,x_i,x})$ for some $x \in B$, and $\ell^{-(1/\epsilon'^2)}|B|/K^2 \leq |T(i)| \leq |B|/K$.

(b) $T(i) \in \Pi^{(1)}_{x_1,\ldots,x_i}$, $|T(i)| \geq |B|/K$, and there exists $x \in T(i)$ such that $\mu_W(T(i)) \leq (2/3)^i$, where $W = W_{\Pi_{x_1,\ldots,x_i},T(i),k,\epsilon}(x)$.

We prove the claim by induction on i. For $i = 0$, (b) of the claim holds by choosing $T(0) = B$. Now assume $i > 0$ and the claim holds for $i-1$. Consider $x_1, \ldots, x_{i-1} \in B$ and $T(i-1) \subseteq B$ satisfying the claim for $i-1$.

First assume (a) holds for $i-1$, i.e., $T(i-1) \in \mathcal{B}(\Pi^{(1)}_{x_1,\ldots,x_{i-1},x})$ for some $x \in B$, and

$$\ell^{-(1/\epsilon'^2)}|B|/K^2 \leq |T(i-1)| \leq |B|/K.$$

Let $x_i = x$ and $x' \in B$. By Lemma 15, $T(i-1) \in \mathcal{B}(\Pi^{(1)}_{x_1,\ldots,x_i,x'})$. Choose $T(i) = T(i-1)$. Then (a) also holds for i.

So assume (b) holds for $i-1$, i.e., $T(i-1) \in \Pi^{(1)}_{x_1,\ldots,x_{i-1}}$, $|T(i-1)| \geq |B|/K > K$, and there exists $x \in T(i-1)$ such that $\mu_W(T(i-1)) \leq (2/3)^{i-1}$, where $W = W_{\Pi_{x_1,\ldots,x_{i-1}},T(i-1),k,\epsilon}(x)$. In particular, $\mu(T(i-1)) \geq |T(i-1)|/|\langle B \rangle| \geq K^{-2}$.

Let $t = 3K^3 \geq \lfloor \frac{3K}{2\mu(T(i-1))} \rfloor + 1$ and $k' = k(t+2)$. Then $m - (i-1) \geq 4k' + 2$. Applying Lemma 50 to $\Pi_{x_1,\ldots,x_{i-1}}$ and $T(i-1)$, we see that either of the following two cases holds:

[3] Lemma 19 shows that, if $|B+B| \gg |B|$, we could find $B' \subseteq B$ with a mild lower bound for $\min\{|B'|, |B|/|B'|\}$. However, in Lemma 51, we need both a lower bound and a (good) upper bound for $|B|/|B'|$, and the latter does not follow from Lemma 19. This upper bound is used in the analysis for the case that $|B|^2/|B+B|$ is small (see the proof of Lemma 17 in Subsection 4.3).

1. There exist $y \in T(i-1)$ and $B' \in \mathcal{B}(\Pi^{(1)}_{x_1,\ldots,x_{i-1},x,y})$ such that $B' \subseteq T(i-1)$ and $\ell^{-(1/\epsilon'^2)}|T(i-1)|/K \leq |B'| \leq |T(i-1)|/K$.
2. There exist $B' \in \Pi^{(1)}_{x_1,\ldots,x_{i-1},x}$ and $y \in B'$ such that $B' \subseteq T(i-1) \cap W$, $|B'| \geq |T(i-1)|/K$, and $\mu_{W'}(B') \leq (\mu_W(T(i-1)) + \epsilon)/2$, where $W' = W_{\Pi_{x_1,\ldots,x_{i-1},x},k,B',\epsilon}(y)$.

In Case (1), let $x_i = x$ and $T(i) = B'$, so that $T(i) \in \mathcal{B}(\Pi^{(1)}_{x_1,\ldots,x_i,y})$. In this case, as $|B|/K \leq |T(i-1)| \leq |B|$, we have $\ell^{-(1/\epsilon'^2)}|B|/K^2 \leq |T(i)| \leq |B|/K$, i.e., (a) holds for i.

Now consider Case (2). Let $x_i = x$ and $T(i) = B'$, so that $T(i) \in \Pi^{(1)}_{x_1,\ldots,x_i}$. We have $|T(i)| \geq |T(i-1)|/K \geq |B|/K^2$. If $|T(i)| \leq |B|/K$ then (a) holds for i. So assume $|T(i)| \geq |B|/K$. By Lemma 44, we have

$$\mu_{W'}(T(i)) \leq (\mu_W(T(i-1)) + \epsilon)/2 \leq ((2/3)^{i-1} + \epsilon)/2 \leq (2/3)^i.$$

So (b) holds for i. This proves the claim.

If (a) holds for $i = r$ then the lemma holds. So we assume (b) holds for $i = r$, i.e., there exist $x_1, \ldots, x_r \in B$, $T(r) \subseteq B$, and $x \in T(r)$ such that $T(r) \in \Pi^{(1)}_{x_1,\ldots,x_r}$, $|T(r)| \geq |B|/K$, and $\mu_W(T(r)) \leq (2/3)^r$, where $W = W_{\Pi_{x_1,\ldots,x_r},T(r),k,\epsilon}(x)$.

In the following, let $\Pi' := \Pi_{x_1,\ldots,x_r}$, $B' := T(r)$, and $W := W_{\Pi_{x_1,\ldots,x_r},T(r),k,\epsilon}(x)$.

Step 2: Reducing the cardinality of a block.

We claim that for $0 \leq i \leq r$, there exist $y_1, \ldots, y_{2i+1} \in B$ and $U(i) \subseteq B' \cap W$ such that $U(i) \in \mathcal{B}(\Pi'^{(1)}_{y_1,\ldots,y_{2i+1}})$ and

$$\ell^{-(1/\epsilon'^2)}|B|/K^3 \leq |U(i)| \leq \max\{K^{-1}, (2\gamma)^i\} \cdot |B|.$$

We prove this claim by induction on i. For $i = 0$, let $y_1 = x$ and $U(0) = B' \cap W$. By Theorem 40 (1), we have $H_{\Pi',B',k,\epsilon} \in \mathcal{B}(\mathcal{S}_{\Pi',t})$ and hence $W \in \mathcal{B}(\mathcal{S}_{\Pi'_{y_1},t+1})$, where $t = 3K^3$ is as chosen in Step 1. By Lemma 35 (1), $B' \cap W \in \mathcal{B}(\Pi'^{(1)}_{y_1})$. By Theorem 40 (4), (5), (6) and the fact $|B'| \geq |B|/K$, we know $|U(0)| = |B' \cap W| \geq \ell^{-(1/\epsilon'^2)}|B|/K$. As $U(0) \subseteq B' \subseteq B$, we also have $|U(0)| \leq |B|$. So the claim holds for $i = 0$.

Now assume $i > 0$ and the claim holds for $i-1$. Consider $y_1, \ldots, y_{2i-1} \in B$ and $U(i-1) \subseteq B' \cap W$ satisfying the claim for $i-1$. If $|U(i-1)| \leq |B|/K$, then the claim holds for i as well by choosing arbitrary $y_{2i}, y_{2i+1} \in B$ and $U(i) = U(i-1)$. So assume $|U(i-1)| > |B|/K$. Then $|U(i-1)| \leq (2\gamma)^{i-1}|B|$.

Next, we prove that the additive energy $E(U(i-1))$ of $U(i-1)$ is less than $\gamma|U(i-1)|^3$. Assume to the contrary that $E(U(i-1)) \geq |U(i-1)|^3$. By Theorem 33, there exist $y \in B$ and $U' \in \mathcal{B}(\Pi'^{(1)}_{y_1,\ldots,y_{2i-1},y})$ such that $U' \subseteq U(i-1)$, $|U'| \geq \gamma|U(i-1)|/3$ and $|U' - U'| < 2^{17}\gamma^{-9}|U(i-1)| \leq 2^{19}\gamma^{-10}|U'|$. It is well known that $\frac{|A+A|}{|A|} \leq \left(\frac{|A-A|}{|A|}\right)^2$ for $A \subseteq V$ (see [37, Exercise 6.5.15]). Therefore,

$$|U' + U'| < (2^{19}\gamma^{-10})^2|U'| = 2^{38}\gamma^{-20}|U'|.$$

By the Freiman–Ruzsa Theorem (Theorem 6), we have

$$\mu(U') > \ell^{-2^{38}\gamma^{-20}}. \tag{12}$$

As $|U'| \geq \gamma|U(i-1)|/3$ and $|U(i-1)| > |B|/K$, we have $|U'| \geq \gamma|B|/(3K) \geq |B|/K^3$. If $|U'| \leq |B|/K$, then the claim holds for i by choosing $y_{2i} = y_{2i+1} = y$ and $U(i) = U'$. So assume $|U'| > |B|/K$. Then the codimension of $\langle U' \rangle$ in $\langle B \rangle$ is at most $\log_\ell(K/\mu(B)) \leq k$. By Theorem 32, $\langle U' \rangle = t(\mathbb{F}U') \in \mathcal{B}(\mathcal{S}_{\Pi'_{y_1,\ldots,y_{2i-1},y},t})$. By definition, $\langle U' \rangle \in \mathcal{W}_{\Pi,k,B}$. So by Lemma 44, we have

$$\mu_{\langle U' \rangle}(B) \leq \mu_W(B) + \epsilon \leq (2/3)^r + (2/3)^{r-1}/3 = (2/3)^{r-1} \leq \ell^{-2^{38}\gamma^{-20}}$$

where the last inequality holds since $\gamma = 4\left((r-1)/\log \ell\right)^{-1/20}$. But this contradicts (12) since $\mu(U') \le \mu_{\langle U'\rangle}(B)$. Therefore, $E(U(i-1)) < \gamma |U(i-1)|^3$.

For $z \in U(i-1)+U(i-1)$, denote by $\nu^+(z)$ the number of $(a,b) \in U(i-1)\times U(i-1)$ satisfying $a+b=z$. Then

$$\sum_{z\in U(i-1)+U(i-1)} \nu^+(z) = |U(i-1)|^2 \quad \text{and} \quad \sum_{z\in U(i-1)+U(i-1)} \nu^+(z)^2 = E(U(i-1)).$$

Note $|U(i-1)+U(i-1)| \le |\langle B\rangle| \le K|B| \le K^2|U(i-1)|$. Let

$$T = \{z \in U(i-1)+U(i-1) : \nu^+(z) \ge |U(i-1)|/(2K^2)\}.$$

Then

$$\begin{aligned}\sum_{z\in T} \nu^+(z) &= \sum_{z\in U(i-1)+U(i-1)} \nu^+(z) - \sum_{z\in (U(i-1)+U(i-1))\setminus T} \nu^+(z)\\ &\ge |U(i-1)|^2 - |U(i-1)+U(i-1)|\cdot |U(i-1)|/(2K^2)\\ &\ge |U(i-1)|^2/2.\end{aligned}$$

On the other hand, $\sum_{z\in T}\nu^+(z)^2 \le E(U(i-1)) < \gamma|U(i-1)|^3$. So there exists $z_0 \in T$ such that

$$\nu^+(z_0) \le \left(\sum_{z\in T}\nu^+(z)^2\right) / \left(\sum_{z\in T}\nu^+(z)\right) \le 2\gamma|U(i-1)| \le (2\gamma)^i|B|.$$

As $z_0 \in T$, we also have

$$\nu^+(z_0) \ge |U(i-1)|/(2K^2) \ge \ell^{-(1/\epsilon'^2)}|B|/K^3.$$

Choose $y_{2i}, y_{2i+1} \in U(i-1)$ such that $y_{2i}+y_{2i+1}=z_0$. Let

$$U(i) = \{a \in U(i-1) : \exists\ b \in U(i-1) \text{ such that } a+b = y_{2i}+y_{2i+1}\}.$$

Then $U(i) \in \mathcal{B}(\Pi'^{(1)}_{y_1,\dots,y_{2i+1}})$ and $|U(i)| = \nu^+(z_0)$. So the claim holds for i.

This proves the claim for all $0 \le i \le r$. The lemma follows by choosing $i=r$. ◀

Now we are ready to prove Lemma 21.

Proof of Lemma 21. Let $K = \ell^{2(\log\log\log N)^{1/2}}$. As $|B+B|/|B| \le (\log\log\log N)^{1/2}$, we have $|\langle B\rangle|/|B| \le K$ by the Freiman–Ruzsa Theorem (Theorem 6). Pick the following parameters:

- $k = 6K^4$,
- $r = \lceil \log K/\log\log K\rceil + 1$,
- $\gamma = 4\left((r-1)/\log\ell\right)^{-1/20}$,
- $\epsilon = (2/3)^{r-1}/3$, and
- $\epsilon' = \epsilon/\ell^k$.

Note $\log\ell \le (\log\log\log\log N)^{1/2}$ by assumption.

As we assume $N \ge c$ for a sufficiently large constant $c>0$, the conditions in Lemma 51 are satisfied. By Lemma 51, there exist $r' = \Theta(r)$, $x_1,\dots,x_{r'} \in B$, and $B' \in \mathcal{B}(\Pi^{(1)}_{x_1,\dots,x_{r'}})$ such that

$$|B|/|B'| \ge \min\{K, (2\gamma)^{-r}\} = 2^{\Theta(r\log\log\log\log N)}$$

and

$$|B|/|B'| \le K^3\ell^{1/\epsilon'^2} = K^3\ell^{\ell^{12K^4}/\epsilon^2} \le 2^{2^{2^{(\log\log\log N)^{1/2+o(1)}}}} \le 2^{\sqrt{\log N}},$$

as desired. ◀