Irredundant hyperplane covers

János Nagy*  Péter Pál Pach†  István Tomon‡

Abstract

We prove that if $G$ is an abelian group and $H_1 x_1, \ldots, H_k x_k$ is an irredundant (minimal) cover of $G$ with cosets, then

$$|G : \bigcap_{i=1}^{k} H_i| = 2^{O(k)}.$$ 

This bound is the best possible up to the constant hidden in the $O(\cdot)$ notation, and it resolves conjectures of Pyber (1996) and Szegedy (2007).

We further show that if $G$ is an elementary $p$-group for some large prime $p$, and $H_1, \ldots, H_k$ is a sequence of hyperplanes with many repetitions, then the bound above can be improved. As a consequence, we establish a substantial strengthening of the recently solved Alon-Jaeger-Tarsi conjecture: there exists $\alpha > 0$ such that for every invertible matrix $M \in \mathbb{F}_p^{n \times n}$ and any set of at most $p^{\alpha}$ forbidden coordinates, one can find a vector $x \in \mathbb{F}_p^n$ such that neither $x$ nor $Mx$ have a forbidden coordinate.

1 Introduction

A covering of a set with a collection of its subsets is irredundant, if no proper subcollection forms a covering. How diversely can a group be covered with its cosets? This question can be traced back to the 50s, when Neumann [11] proved that if $G$ is a group and $H_1 x_1, \ldots, H_k x_k$ is an irredundant covering of $G$ with cosets, then $|G : \bigcap_{i=1}^{k} H_i|$ is finite. In [12], he further proved that this index can be bounded by some function of $k$. Therefore, it makes sense to define $f(k)$, the smallest integer which satisfies $|G : \bigcap_{i=1}^{k} H_i| \leq f(k)$ for every group $G$ and every irredundant covering with $k$ cosets. It was only in 1987 when Tomkinson [16] determined the precise value $f(k) = k!$, where the equality is achieved by a certain coset cover of the symmetric group $S_k$.

Tomkinson further proposed to study the problem of covering with subgroups instead of cosets. To this end, let $g(k)$ denote the smallest integer which satisfies $|G : \bigcap_{i=1}^{k} H_i| \leq g(k)$ for every group $G$ and every irredundant covering $H_1, \ldots, H_k$ with subgroups. Clearly, $g(k) \leq f(k)$. Tomkinson [16] proved that $g(k) \geq \frac{1}{2} 3^{2(n-1)/3}$, while the best known upper bound improves $k!$ by only a polynomial factor. The lack of constructions suggests that perhaps $g(k) = 2^{O(k)}$ should be the truth.

*Alfréd Rényi Institute of Mathematics;
Department of Computer Science and Information Theory, Budapest University of Technology and Economics, Műegyetem rkp. 3., H-1111 Budapest, Hungary;
MTA-BME Lendület Arithmetic Combinatorics Research Group, ELKH, Műegyetem rkp. 3., H-1111 Budapest, Hungary., email: janomo4@gmail.com

†Department of Computer Science and Information Theory, Budapest University of Technology and Economics, Műegyetem rkp. 3., H-1111 Budapest, Hungary;
MTA-BME Lendület Arithmetic Combinatorics Research Group, ELKH, Műegyetem rkp. 3., H-1111 Budapest, Hungary., email: ppp@cs.bme.hu

‡ETH Zurich, e-mail: istvan.tomon@math.ethz.ch
Pyber [14] observed that in case $G$ is an elementary $p$-group, the latter question is closely related to the problem of covering a group with abelian subgroups. He conjectured that an exponential upper bound should hold at least in this case. See e.g. [13] for further details about the problem of covering with abelian subgroups. To this end, define $f_A(k)$ and $g_A(k)$ the same way as $f(k)$ and $g(k)$, respectively, with the additional restriction that $G$ is abelian. Szegedy [15] conjectured that $f_A(k) = 2^{O(k)}$ might also be true, immediately implying $g_A(k) = 2^{O(k)}$ and the conjecture of Pyber as well. The first significant improvement on the bound $f_A(k) \leq f(k) = k!$ is due to a recent result of the present authors [9], who proved that $f_A(k) = 2^{O(k \log \log k)}$. In this paper, we further refine the methods of [9] with the introduction of certain probabilistic ideas involving Markov chain processes, and settle the conjecture of Szegedy, and thus the conjecture of Pyber as well.

**Theorem 1.1.** Let $G$ be an abelian group and let $H_1 x_1, \ldots, H_k x_k$ be an irredundant covering of $G$ with cosets. Then

$$|G : \bigcap_{i=1}^k H_i| \leq 2^{O(k)}.$$ 

This bound is also the best possible up to the constant factor hidden in the $O(\cdot)$ notation. Indeed, one can take $G = \mathbb{F}_2^{k-1}$, $H_i x_i = \{y \in G : y(i) = 1\}$ for $i \in [k-1]$ and $H_k x_k = \{0\}$; this gives $|G : \bigcap_{i=1}^k H_i| = 2^{k-1}$. One of the most interesting subcases of Theorem 1.1 is when $G = \mathbb{F}_p^n$ is an elementary $p$-group, and every coset in the covering is maximal, in other words, each coset is a hyperplane. This special subcase has the following equivalent formulation.

**Theorem 1.2.** Let $p$ be a prime, $n, N$ be positive integers, and let $H_1, \ldots, H_N < \mathbb{F}_p^n$ be hyperplanes such that $H_1 + v_1, \ldots, H_N + v_N$ is an irredundant covering of $\mathbb{F}_p^n$ for some $v_1, \ldots, v_N \in \mathbb{F}_p^n$. Then

$$\text{codim} \left( \bigcap_{i \in [N]} H_i \right) = O \left( \frac{N}{\log p} \right).$$

Note that the upper bound $\text{codim} \left( \bigcap_{i \in [N]} H_i \right) \leq N$ is straightforward, however, proving any upper bound of the form $N(1 - \epsilon(p))$ with $\epsilon(p) > 0$ depending only on $p$ is already highly nontrivial. Szegedy [15] observed that this problem is closely related to several longstanding conjectures in linear algebra, namely the Alon-Jaeger-Tarsi conjecture [3, 7] on non-vanishing linear maps, and the Additive Basis conjecture [2]. More precisely, Szegedy [15] showed that Theorem 1.2 implies the Alon-Jaeger-Tarsi conjecture for large primes (in fact, having $\epsilon(p) > 1/2$ is sufficient), which was recently settled by the first and the second named authors [8], while it implies certain weak versions of the Additive Basis conjecture, see [9] for recent progress.

However, we have no reason to believe that Theorem 1.2 is also sharp for large primes $p$. In case there are many repetitions among $H_1, \ldots, H_N$, we can indeed achieve some improvement.

**Theorem 1.3.** Let $p$ be a prime, and $n, M, r$ be positive integers, $r \geq 2$. Let $H_1, \ldots, H_M < \mathbb{F}_p^n$ be hyperplanes such that there exists an irredundant covering of $\mathbb{F}_p^n$ using at most $r$ translates of each of $H_1, \ldots, H_M$. Then

$$\text{codim} \left( \bigcap_{i=1}^M H_i \right) = O \left( \frac{M \log r}{\log p} \right).$$

(To clarify, if a hyperplane appears $k$ times in the sequence $H_1, \ldots, H_M$, we are allowed to take $kr$ translates of it in total.)
Note that in the theoretically best case, when the irredundant cover contains $N = \Omega(rM)$ hyperplanes, Theorem 1.3 gives an $O(\log r/r)$ factor improvement over Theorem 1.2. This result is motivated by applications about the choosability version of the Alon-Jaeger-Tarsi conjecture, proposed by DeVos [5]. For a prime $p$, let $h(p)$ denote the largest $k$ such that for every $A \subset \mathbb{F}_p$ of size $k$, and every invertible matrix $M \subset \mathbb{F}_p^{n \times n}$, there exists $x \in \mathbb{F}_p^n$ such that neither $x$, nor $Mx$ has a coordinate in $A$. The original version of the Alon-Jaeger-Tarsi conjecture [3, 7] is implied by the statement $h(p) \geq 1$. In [8, 9], it is proved that $h(p) = \Omega(\log p/\log \log p)$ if $p$ is sufficiently large (see Theorem 5.1 in [9]). A direct reduction from Theorem 1.2 gives the slight improvement $h(p) = \Omega(\log p)$, while Theorem 1.3 significantly strengthens this.

**Theorem 1.4.** There exists an absolute constant $\alpha > 0$ such that the following holds for every sufficiently large prime $p$ and integer $n$. Let $A \subset \mathbb{F}_p$ such that $|A| < p^\alpha$, and let $M \in \mathbb{F}_p^{n \times n}$ be an invertible matrix. Then there exists $x \in \mathbb{F}_p^n$ such that neither $x$, nor $Mx$ has a coordinate in $A$.

We remark that the slightly more general version in which we individually forbid a set of elements for each coordinate of $x$ and $Mx$, also holds. That is, if $A_1, \ldots, A_n, B_1, \ldots, B_n \subset \mathbb{F}_p$ are sets, each of size at most $p^\alpha$, then there exists $x$ such that $x(i) \notin A_i$ and $(Mx)(i) \notin B_i$ for $i \in [n]$.

Theorem 1.1 is also closely related to the classical result of Alon and Füredi [1] which states that if $h_1, \ldots, h_n$ are positive integers, and one wants to cover all but exactly one point of the finite grid $\{x \in \mathbb{Z}^n : \forall i \in [n], 0 \leq x(i) \leq h_i\}$ with hyperplanes (over the real numbers), then one needs at least $h_1 + \cdots + h_n$ hyperplanes, and this bound is the best possible. An analogue of this for coset covers of abelian groups is proved by Szegedy [15]: if $G$ is an abelian group and $|G| = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ is the prime factorization of $|G|$, then any collection of cosets covering all but one point of $G$ has at least $\sum_{i=1}^r \alpha_i (p_i - 1)$ elements, and this bound is the best possible. This shows that if an irredundant covering $H_1 x_1, \ldots, H_k x_k$ of $G$ contains a one element set, in which case we also have $|G : \bigcap_{i \in [k]} H_i| = |G|$, then $k \geq 1 + \sum_{i=1}^r \alpha_i (p_i - 1)$. Note that, however, an irredundant covering of $G$ with $|G : \bigcap_{i \in [k]} H_i| = |G|$ can have fewer elements. Indeed, if $p \geq 3$ and $G = \mathbb{F}_p^2$, the collection of all lines containing the origin is such a covering with $p + 1 < 2(p - 1) + 1$ elements.

In this paper, we build on the developments of [8] and [9] to prove Theorem 1.1. We follow closely the approach of these papers, but introduce crucial new ideas as well. Interestingly, our proof combines linear algebraic, combinatorial, and probabilistic techniques alike. In the next section, we introduce some notation, outline our proof, and recall the key results from [9]. Then, we present our main contribution and the proof of the main theorem in Section 3. In Section 4, we prove Theorems 1.3 and 1.4. We finish our paper with some remarks about numerical results.

## 2 Preliminaries

Let us introduce some notation. Given a prime $p$, an integer $n$, $v \in \mathbb{F}_p^n$ and $t \in \mathbb{F}_p$, let $H_{p,n}(v,t)$ denote the hyperplane $\{x \in \mathbb{F}_p^n : \langle v,x \rangle + t = 0\}$. If $p$ and $n$ are clear from the context, we simply write $H(v,t)$.

Given a multiset of vectors $V \subset \mathbb{F}_p^n$, let

$$\ker(V) = \left\{ w \in \mathbb{F}_p^n : \sum_{v \in V} w(v)v = 0 \right\},$$

and let $\dim(V)$ be the dimension of the vector space spanned by the elements of $V$. Note that

$$\dim(V) + \dim(\ker(V)) = |V|.$$
2.1 Outline of the proofs

Let us outline the approach of [9], which we also closely follow. It turns out that in order to prove Theorem 1.1, it is enough to prove Theorem 1.2. The latter is equivalent with following: if $V \subset \mathbb{F}_p^n$ is a multiset and $\{H(v, t_v)\}_{v \in V}$ is an irredundant covering of $\mathbb{F}_p^n$, then $|V| = \Omega(\dim(V) \log p)$.

In order to prove this, we establish a connection between irredundant covers with hyperplanes and certain products in the group ring $\mathbb{C}[\mathbb{F}_p^n]$ vanishing. More precisely, we show that the collection of hyperplanes $\{H(v, t_v)\}_{v \in V}$ is a covering of $\mathbb{F}_p^n$ if and only if the equality

$$\prod_{v \in V} (1 - e^{2\pi i v_i/p} g^v_i) = 0$$

holds in the group ring $\mathbb{C}[\mathbb{F}_p^n]$.

By studying the coefficients of the terms $g^u$ for $u \in \mathbb{F}_p^n$ on the left hand side of (1), we establish the following combinatorial property of $\ker(V)$. For every $w \in \mathbb{F}_p^n$ with no zero coordinates and every $v_0 \in V$, there exists some $w' \in \ker(V)$ such that $w'(v_0) = w(v_0)$ and $w'(v) \in \{-w(v), 0, w(v)\}$ for $v \in V$. We call subspaces with this property versatile.

We finish the proof by finding a lower bound on the dimension of versatile subspaces. In [9], it was shown (essentially) that if $W < \mathbb{F}_p^N$ is versatile, then $\dim(W) \geq (1 - O(\log \log p/\log p))N$. Also, this bound is the limit of the method presented in [9]. The main contribution of this manuscript is a novel approach of bounding the dimension of versatile subspaces, which ultimately lets us show that the $\log \log p$ factor can be removed. This lower bound on $\dim(\ker(V))$ combined with the equality $\dim(\ker(V)) = |V| - \dim(V)$ implies the desired inequality $|V| = \Omega(\dim(V) \log p)$.

In order to prove Theorem 1.3, we study the additional constraints imposed on $\ker(V)$ due to the repeated elements.

In the next sections, we recall a number of key definitions and results from [9]. First, we start with a brief introduction to group rings.

2.2 Group rings

In this section, we recall several results about the group ring $\mathbb{C}[\mathbb{F}_p^n]$, and establish the connection between hyperplane covers and group ring products. But first, let us formally introduce the notion of group ring.

Given an additive group $G$ and a ring $R$, the group ring $R[G]$ is the ring of formal expressions $\sum_{v \in G} r_v g^v$, where $r_v \in R$, and $g$ is a formal variable. Addition and multiplication are defined in the natural way, that is,

$$\left( \sum_{v \in G} r_v g^v \right) + \left( \sum_{v \in G} r'_v g^v \right) = \sum_{v \in G} (r_v + r'_v) g^v,$$

and

$$\left( \sum_{v \in G} r_v g^v \right) \cdot \left( \sum_{v \in G} r'_v g^v \right) = \sum_{v \in G} \left( \sum_{w \in G} r_w r'_v \delta_{v, w} \right) g^v.$$

Note that an element $h = \sum_{v \in G} r_v g^v \in R[G]$ corresponds to the function $h^* : G \rightarrow R$ defined as $h^*(v) = r_v$. Then, the product $h_1 \cdot h_2$ corresponds to the convolution $h_1^* * h_2^*$.

The following is a definition.
Definition 1. A multiset of vectors $V \subset \mathbb{F}_p^n$ is irredundant if for each $v \in V$ there exists $t_v \in \mathbb{F}_p$ such that in the group ring $\mathbb{C}[\mathbb{F}_p^n]$, we have
\[
\prod_{v \in V} (1 - e^{2\pi i t_v/p} g_v^v) = 0,
\]
but for every $w \in V$,
\[
\prod_{v \in V \setminus \{w\}} (1 - e^{2\pi i t_v/p} g_v^v) \neq 0.
\]

The next lemma connects irredundant sets of vectors with irredundant hyperplane covers. Its proof is contained in the proof of Lemma 4.2 in [9], but for completeness, we also present it here.

Lemma 2.1. Let $V \subset \mathbb{F}_p^n$ be a multiset. Then some translates of the hyperplanes $H(v,0)$ for $v \in V$ form an irredundant cover of $\mathbb{F}_p^n$ if and only if $V$ is irredundant.

Proof. For $v \in \mathbb{F}_p^n$ and $t \in \mathbb{F}_p$, let $h_{v,t} = 1 - e^{2\pi i t/p} g_v^v \in \mathbb{C}[\mathbb{F}_p^n]$. Then $h_{v,t}^* : \mathbb{F}_p^n \to \mathbb{C}$ is the function defined as $h_{v,t}^*(0) = 1$, $h_{v,t}^*(v) = -e^{2\pi i t/p}$, and $h_{v,t}^*(x) = 0$ otherwise. Consider the discrete Fourier transform of $h_{v,t}^*$, denoted as $F(h_{v,t}^*)$. It is easy to calculate that $F(h_{v,t}^*)(y) = 1 - e^{2\pi i t/(y,v)}$ for every $y \in \mathbb{F}_p^n$. But then the set of vectors on which $F(h_{v,t})$ vanishes is exactly the hyperplane $H(v,t)$.

Therefore, if for each $v \in V$ we assign some $t_v \in \mathbb{F}_p^n$, then the hyperplanes $H(v,t_v)$ for $v \in V$ form a covering of $\mathbb{F}_p^n$ if and only if
\[
\prod_{v \in V} F(h_{v,t_v}^*) = 0.
\]
This is equivalent to the convolution of the functions $h_{v,t_v}^*$ for $v \in V$ being 0, which is further equivalent to $\prod_{v \in V} h_{v,t} = 0$. Therefore, $V$ is irredundant if and only if some translates of the hyperplanes $H(v,0)$ for $v \in V$ form an irredundant cover of $\mathbb{F}_p^n$.

Note that being an irredundant set of vectors is a projective property. That is, if $V \subset \mathbb{F}_p^n$ is irredundant, then after scaling the elements of $V$ arbitrarily, the resulting set is also irredundant. This follows trivially, for instance, from the previous lemma.

By studying the coefficients in the product $\prod_{v \in V} (1 - e^{2\pi i t_v/p} g_v^v) = 0$, combined with the previous observation, one can deduce the following combinatorial property of $\ker(V)$ in case $V$ is irredundant.

Definition 2. A subspace $W < \mathbb{F}_p^N$ is versatile if for every $x \in \mathbb{F}_p^n$ with no zero coordinates and every index $j \in [N]$ there exists $w \in W$ such that $w(i) \in \{-x(i), 0, x(i)\}$ for every $i \in [N]$, and $w(j) = x(j)$.

Lemma 2.2. ([9], Lemma 2.5 for $r = 1$) Let $V \subset \mathbb{F}_p^n$ be an irredundant multiset, then $\ker(V)$ is versatile.

2.3 Abelian groups

In this section, we show how to reduce Theorem 1.1 to the special case when $G = \mathbb{F}_p^n$, and all cosets in the cover are hyperplanes. For an abelian group $G$, define $\phi(G)$ to be the minimal $k$ such that $G$ has an irredundant covering $H_1 x_1, \ldots, H_k x_k$ with $k$ cosets where $\bigcap_{i=1}^k H_i$ is trivial. Furthermore, for a prime $p$ and integer $n$, let $\phi(p,n)$ denote the smallest $k$ such that for some multiset $V \subset \mathbb{F}_p^n$ of size $k$ satisfying $\dim(V) = n$, there is an irredundant covering with hyperplanes $H(v,t_v)$ for $v \in V$. Finally, set $\lambda_p = \inf_{n \to \infty} \phi(p,n)^{-1}$, and for $N = p_1^{\ell_1} \cdots p_\ell^{\ell_\ell}$, where $p_1, \ldots, p_\ell$ are distinct primes, let
\[
\lambda(N) = \sum_{i=1}^\ell n_i \lambda_{p_i}.
\]
Lemma 2.3. ([9], Lemma 4.6) Let $G$ be a finite abelian group. Then $\phi(G) \geq \lambda(|G|) + 1$.

Finally, for small primes $p$, we use the following result.

Lemma 2.4. (Szegedy [15]) For every prime $p$ and $n \in \mathbb{N}^+$, we have $\phi(p, n) \geq n + 1$. Thus, $\lambda_p \geq 1$.

With this, we recalled all the results from [9] needed for our proof. In what comes, we present new tools and ideas.

2.4 Markov chains

Our proof relies on some light probability theory. More precisely, we use some basic results about Markov chains, which we state in this section for convenience.

Let $X_0, X_1, \ldots$ be a regular Markov chain on a finite state space $\Omega$ with transfer matrix $P$. That is, for $t \in \mathbb{N}$ and $x, y \in \Omega$, we have

$$
P(X_{t+1} = y | X_t = x) = P(x, y).
$$

From this, if $\mu : \Omega \to [0, 1]$ is the distribution of $X_0$, then $\mu P^t$ is the distribution of $X_t$. Say that $P$ is irreducible if for every $x, y \in \Omega$ there exists $t \in \mathbb{N}$ such that $P^t(x, y) > 0$. Also, say that $P$ is aperiodic if for every $x \in \Omega$, the greatest common divisor of the elements of the set $\{t \in \mathbb{N}^+ : P^t(x, x) > 0\}$ is 1. We use the following lemma about the convergence of distributions in a Markov chain.

Lemma 2.5. ([6]) Let $P$ be an irreducible, aperiodic transfer matrix. Then there is a unique distribution $\pi$ satisfying $\pi P = \pi$, called the stationary distribution. Furthermore, there exists $0 < \alpha < 1$ and $C > 0$ such that for every distribution $\mu$ on $\Omega$, we have

$$
\max_{A \subseteq \Omega} |\pi(A) - (\mu P^t)(A)| \leq C \alpha^t.
$$

3 Versatile subspaces

In this section, we present our main contribution, which can be stated as the following lemma.

Lemma 3.1. There exists an absolute constant $c > 0$ such that for every prime $p$ and positive integer $N$, if $W \subset \mathbb{F}_p^N$ is versatile, then

$$
\dim(W) \geq \left(1 - \frac{c}{\log p}\right)N.
$$

Say that a set $A \subset \mathbb{F}_p$ is arithmetic, if each element of $A$ is the middle element of a nontrivial 3-term arithmetic progression contained in $A$. In [9], it was proved (essentially) that if $A \subset \mathbb{F}_p$ is arithmetic and $W \subset \mathbb{F}_p^N$ is versatile, then $W + A^N = \mathbb{F}_p^N$. As the size of the smallest arithmetic set is $(1+o(1)) \log_2 p$, see [4, 10], this implies $|W| \geq p^{N/2} \geq p^N(1-O(\log \log p/\log p))$ and $\dim(W) \geq N(1 - O(\log \log p/\log p))$.

In order to improve this, we replace the set $A^N$ with some carefully constructed much smaller set $H \subset \mathbb{F}_p^N$ which still satisfies $W + H = \mathbb{F}_p^N$.

Let us observe that if $W_1 \subset \mathbb{F}_p^{N_1}$ and $W_2 \subset \mathbb{F}_p^{N_2}$ are both versatile, then $W_1 \oplus W_2 = \{(w_1, w_2) : w_1 \in W_1, w_2 \in W_2\} \subset \mathbb{F}_p^{N_1+N_2}$ is also versatile. Therefore, if there exists a versatile subspace of $\mathbb{F}_p^{N_0}$ of dimension $\alpha N_0$, then there exists a versatile subspace of $\mathbb{F}_p^N$ of dimension $\alpha N$ for every $N$ divisible by $N_0$. This implies that it is enough to prove Lemma 3.1 in case $N$ is sufficiently large with respect to $p$, which we restate as follows.
Lemma 3.2. There exists an absolute constant \( c > 0 \) such that for every prime \( p \) and positive integer \( N \), where \( N \) is sufficiently large with respect to \( p \), if \( W < \mathbb{F}_p^N \) is versatile, then

\[
\dim(W) \geq \left(1 - \frac{c}{\log p}\right)N.
\]

First, let us define our set \( H \subset \mathbb{F}_p^N \). To this end, let us introduce some further notation. Let \( \tau : \mathbb{F}_p \to \mathbb{N} \cup \{\infty\} \) be the function defined as follows: \( \tau(0) = 0 \), and if \( b \neq 0 \), then \( \tau(b) \) is the smallest nonnegative integer \( r \) such that \( 2^r \in \{-b, b\} \); if there exists no such \( r \), then set \( \tau(b) = \infty \). Let \( \Omega \subset \mathbb{F}_p \) be the set of elements \( b \) such that \( \tau(b) < \infty \).

For \( x \in \mathbb{F}_p^N \) and \( b \in \mathbb{F}_p \), let \( S(b, x) \) denote the number of coordinates of \( x \) equal to \( b \). Finally, let \( H \subset \mathbb{F}_p^N \) be the set of vectors \( x \) for which

\[
S(b, x) \leq \frac{100(\tau(b) + 1)^2}{2\tau(b)} N
\]

holds for every \( b \in \mathbb{F}_p \); by convention, \( S(b, x) = 0 \) if \( b \notin \Omega \). First, let us bound the size of \( H \).

Claim 3.3. There exists a constant \( c' > 0 \) such that if \( N \) is sufficiently large with respect to \( p \), then \( |H| \leq 2^{c'N} \).

Proof. For \( b \in \mathbb{F}_p \), let \( n_b \) be a nonnegative integer such that \( \sum_{b \in \mathbb{F}_p} n_b = N \). Then the number of vectors \( x \in \mathbb{F}_p^N \) such that \( S(b, x) = n_b \) for every \( b \in \mathbb{F}_p \) is

\[
\prod_{b=0}^{p-1} \binom{N - \sum_{i=0}^{n_b-1} n_i}{n_b} \leq \prod_{b=0}^{p-1} \binom{N}{n_b} < \prod_{b=0}^{p-1} \left(\frac{eN}{n_b}\right)^{n_b}.
\]

If \( n_b \leq \frac{100(\tau(b) + 1)^2}{2\tau(b)} N \leq N \) holds, we can write

\[
\left(\frac{eN}{n_b}\right)^{n_b} \leq \left(\frac{e2^{\tau(b)}}{100(\tau(b) + 1)^2}\right)^{100(\tau(b) + 1)^2 2^{-\tau(b)} N} < 2^{100(\tau(b) + 1)^2 3^{-\tau(b)} N},
\]

where the first inequality follows by noting that the function \( f(x) = (eN/x)^x \) is monotone increasing for \( x \in [0, N] \). As \( f(x) \) attains its maximum at \( x = N \), \( (eN/n_b)^{n_b} < e^N \) holds for every \( n_b > 0 \), so (3) holds even if \( N < \frac{100(\tau(b) + 1)^2}{2\tau(b)} N \). Hence, if \( n_b \leq \frac{100(\tau(b) + 1)^2}{2\tau(b)} N \) for every \( b \in \mathbb{F}_p \), we can further bound the right hand side of (2) by

\[
\prod_{b \in \mathbb{F}_p} 2^{100(\tau(b) + 1)^2 3^{-\tau(b)} N} \leq \prod_{r=0}^{\infty} 2^{200(r + 1)^3 2^{-r} N} < 2^{c'' N}
\]

for some constant \( c'' > 0 \), where the first inequality holds after noting that for each \( r \in \{0, \ldots, p - 1\} \), the equation \( \tau(b) = r \) has at most 3 solutions (3 solutions if \( r = 0 \), and at most 2 otherwise). As the number of choices for the partition \( N = \sum_{b \in \mathbb{F}_p} n_b \) is at most \( N^p \), we get \( |H| \leq N^p 2^{c'' N} < 2^{c' N} \) for some suitable constant \( c' > 0 \), assuming \( N \) is sufficiently large with respect to \( p \).  

In what comes, we show that \( W + H = \mathbb{F}_p^N \). This immediately implies Lemma 3.2, as then

\[
|W| \geq \frac{p^N}{|H|} \geq p^N 2^{-c' N},
\]

so \( \dim(W) \geq (1 - c/\log p)N \) with \( c = c' \log 2 \). Therefore, the following claim concludes our proof.
Claim 3.4. For every $x \in \mathbb{F}_p^N$ there exists $w \in W$ such that $x + w \in H$.

Proof. Define the random sequence of vectors $x = x_0, x_1, \ldots$ as follows. For $I \in \mathbb{N}$, let $x_I$ denote the vector we get after changing the 0 coordinates of $x_I$ to 1. Let $j \in [N]$ be the unique index congruent to $I$ modulo $N$. As $W$ is versatile, there exists $w \in W$ such that $w(i) \in \{-x_I^+(i), 0, x_I^+(i)\}$ for $i \in [N]$ and $w(j) = x_I^+(j)$. With probability $1/2$, set either $x_{I+1} = x_I + w$ or $x_{I+1} = x_I - w$. Noting that $x_I - x_0 \in W$ for every $I \in \mathbb{N}$, it is enough to show that if $I$ is sufficiently large, then $P(x_I \in H) > 0$.

Fix some index $k \in [N]$, and consider the sequence $X = (x_0(k), x_1(k), \ldots)$. Then for $I \in \mathbb{N}$, either
(i) $x_{I+1}(k) = x_I(k)$, otherwise,
(ii) if $x_I(k) \neq 0$, then with probability $1/2$, $x_{I+1}(k)$ is either $2x_I(k)$ or 0,
(iii) if $x_I(k) = 0$, then with probability $1/2$, $x_{I+1}(k)$ is either 1 or $-1$.

Let $Y = (Y_0, Y_1, \ldots)$ be the subsequence $(x_{I_0}(k), x_{I_1}(k), \ldots)$ of $X$ such that $I_0 = 0$ and $x_{I_1}(k) \neq x_{I_0}(k)$ for $j \in \mathbb{N}$. Note that for every index $I$, $Y$ contains at least $|I/N|$ elements of $(x_0(k), \ldots, x_I(k))$, as $Y$ contains $x_{I}(k)$ for every $j - 1 \equiv k \pmod{N}$. Furthermore, if $Y_t = 0$ for some $t \in \mathbb{N}$, then $Y_t \in \Omega$ for every $t' > t$. The probability that none of $Y_0, Y_1, \ldots, Y_t$ is equal to 0 is at most $(1/2)^t$. Let $t_0$ be the smallest index such that $Y_{t_0} = 0$, and let $Y' = (Y_{t_0}, Y_{t_0+1}, \ldots)$. Then $Y'$ is a regular Markov chain on the state space $H$, whose transfer matrix $P$ is defined as

- $P(x, 0) = P(x, 2x) = 1/2$ for every $x \in \Omega \setminus \{0\}$,
- $P(0, 1) = P(0, -1) = 1/2$,
- $P(x, y) = 0$ otherwise.

It is easy to check that $P$ is irreducible and aperiodic, so for every probability distribution $\mu$ on $\Omega$, $\mu P^t$ converges to the stationary distribution $\pi$, which is the solution of $\pi P = \pi$. More precisely, by Lemma 2.5, there exist $0 < \alpha < 1$ and $C > 0$ such that $|\mu P^t(x) - \pi(x)| \leq C \alpha^t$ for every $x \in \Omega$. Hence, for every $\epsilon > 0$ there exists $t_1(\epsilon)$ such that if $t_1 \geq t_1(\epsilon)$, then the distribution of $Y_{t_0 + t_1}$ is within $\epsilon$ of $\pi$.

Now let us approximate the stationary distribution $\pi$. For $b \in \Omega \setminus \{-1, 0, 1\}$, we have $\pi(b) = \pi(b/2)/2$. From this, we get $\pi(b) \leq 2^{-\tau(b)}$, which incidentally also holds for $b \in \{-1, 0, 1\}$. Set $\epsilon = 2^{-p}$ and let $t_1 = \max\{t_1(\epsilon), \log_2(2N), \log_2(1/\epsilon)\}$. Then for $b \in \Omega$, we have

$$P(Y_{t_0 + t_1} = b) < \pi(b) + \epsilon \leq 2^{-\tau(b)} + \epsilon.$$ 

Filtering by the event $t_1 \geq t_0$, we can also write

$$P(Y_{2t_1} = b) \leq P(Y_{2t_1} = b|t_1 \geq t_0) + P(t_1 < t_0) < 2^{-\tau(b)} + \epsilon + 2^{-t_1} < 2^{-\tau(b) + 1}.$$ 

On the other hand, we have

$$P(Y_{2t_1} \notin \Omega) \leq 2^{-2t_1} < \frac{1}{2N}.$$ 

Set $z := x_{2t_1 \cdot N}$. Then for each $b \in \Omega$, we have

$$\mathbb{E}(S(b, z)) = \sum_{k \in [N]} P(z(k) = b) \leq 2^{-\tau(b) + 1} N,$$

and for each $k \in [N]$,

$$P(z(k) \notin \Omega) < \frac{1}{2N}.$$
From the latter, we deduce that with probability more than 1/2, every coordinate of \( z \) is in \( \Omega \). For \( b \in \Omega \), let \( A_b \) be the event that \( S(b, z) > 100(\tau(b) + 1)^2 \cdot 2^{-\tau(b)} N \geq 50(\tau(b) + 1)^2 \cdot \mathbb{E}(S(b, z)) \). Applying Markov’s inequality,

\[
P(A_b) \leq \frac{1}{50(\tau(b) + 1)^2}.
\]

Therefore, the probability that \( A_b \) holds for some \( b \in \Omega \) is

\[
P \left( \bigcup_{b \in \Omega} A_b \right) \leq \sum_{b \in \Omega} P(A_b) \leq \sum_{b \in \Omega} \frac{1}{50(\tau(b) + 1)^2} < \frac{3}{50} \sum_{i=1}^{\infty} i^{-2} < \frac{1}{2}.
\]

In conclusion, with positive probability, \( S(b, z) \leq 100(\tau(b) + 1)^2 \cdot 2^{-\tau(b)} N \) holds for every \( b \in \Omega \), and every coordinate of \( z \) is in \( \Omega \). Thus, \( z \in H \) with positive probability.

\( \square \)

This concludes the proof of Lemma 3.1. Now let us put everything together to prove our main theorem.

**Proof of Theorem 1.1.** Let us recall that \( \varphi(p, n) \) denotes the smallest \( k \) such that for some multiset \( V \subset \mathbb{F}_p^n \) of size \( k \) satisfying \( \dim(V) = n \), there is an irredundant covering with hyperplanes \( H(v, t_v) \) for \( v \in V \). Also, \( \lambda_p = \inf_{n \to \infty} \frac{\varphi(p, n)-1}{n} \).

First, let us bound \( \lambda_p \). To this end, let \( V \subset \mathbb{F}_p^n \) be a multiset such that the hyperplanes \( H(v, t_v) \) for \( v \in V \) form an irredundant covering for some choices \( t_v \in \mathbb{F}_p \). Then \( V \) is irredundant by Lemma 2.1. Furthermore,

\[
\dim(\ker(V)) = |V| - \dim(V),
\]

and \( \ker(V) \) is versatile by Lemma 2.2. By Lemma 3.1,

\[
\dim(\ker(V)) \geq |V| \left( 1 - \frac{c}{\log p} \right).
\]

Comparing the two bounds on \( \dim(\ker(V)) \), we get \( |V| \geq \frac{1}{c} \dim(V) \log p \). This gives \( \varphi(p, n) \geq \frac{n}{c} \log p \). Combining this with Lemma 2.4, we get \( \lambda_p \geq \max\{1, \frac{\log p}{c} - 1\} \). Hence, there exists \( \varepsilon > 0 \) such that \( \lambda_p \geq \varepsilon \log p \).

Let \( G \) be an abelian group and let \( H_1 x_1, \ldots, H_k x_k \) be an irredundant covering of \( G \) with cosets. Let \( A = \bigcap_{i=1}^k H_i, \) \( G' = G/A \), and write \( |G'| = p_1^{n_1} \cdots p_\ell^{n_\ell} \), where \( p_1, \ldots, p_\ell \) are distinct primes. Note that \( (H_1/A)x_1, \ldots, (H_k/A)x_k \) is an irredundant covering of \( G' \) with \( \bigcap_{i=1}^k (H_i/A) \) being trivial, so \( k \geq \varphi(G') \).

But then by Lemma 2.3, we have

\[
k \geq \varphi(G') > \lambda(|G'|) = \sum_{i=1}^\ell n_i \lambda_{p_i} \geq \sum_{i=1}^\ell \epsilon n_i \log p_i = \epsilon \log |G'|.
\]

From this, \( |G : \bigcap_{i=1}^k H_i| = |G'| < e^{k/\epsilon} \), finishing the proof.

\( \square \)

## 4 Versatile subspaces with restrictions

In this section, we prove Theorems 1.3 and 1.4. We deduce Theorem 1.3 from the following strengthening of Lemma 3.1.
Lemma 4.1. There exists an absolute constant $c > 0$ such that the following holds. Let $p$ be a prime, $r, M, N$ be positive integers, $r \geq 2$. Let $W < \mathbb{F}_p^N$ be a versatile subspace for which there exists a partition $I_1, \ldots, I_M$ of $[N]$ such that $|I_j| \leq r$ and $\{x \in \mathbb{F}_p^N : \sum_{i \in I_j} x(i) = 0\} < W$ for $j \in [M]$. Then

$$\dim(W) \geq N - \frac{c \log r}{\log p} M.$$ 

Similarly as before, it is enough to prove this theorem in case $M$ is sufficiently large with respect to $p$. Indeed, suppose that $W < \mathbb{F}_p^N$ is a versatile subspace with a suitable partition $I_1 \cup \cdots \cup I_M = [N]$, and $\dim(W) = N - \alpha M$ for some $\alpha \geq 0$. Then for every positive integer $k$, $W' = \oplus_{i=1}^k W < \mathbb{F}_p^{kN}$ is versatile with the suitable partition $I_1 \cup \cdots \cup I_{kM} = [kN]$, where $I_{iM+j} = \{a + iN : a \in I_j\}$ for $i \in [0, k-1], j \in [M]$, and $\dim(W') = k \dim(W) = kN - \alpha kM$.

For a vector $x \in \mathbb{F}_p^N$, define $\nu(x) \in \mathbb{F}_p^M$ such that $\nu(x)(j) = \sum_{i \in I_j} x(i)$ for $j \in [M]$. Also, define $\pi(x) \in \mathbb{F}_p^N$ such that for $j \in [M]$, $\pi(x)(\min I_j) = \nu(x)(j)$ and $\pi(x)(i) = 0$ for $i \in I_j \setminus \{\min I_j\}$. That is, among the indices in $I_j$, we replace the first coordinate with the sum of the coordinates in $I_j$, and set the other coordinates to 0. It is clear that $x - \pi(x) \in W$ for all $x \in \mathbb{F}_p^N$.

Let $H$ be the set defined in Section 3. By Claim 3.4, we have $W + H = \mathbb{F}_p^N$. But then we also have $W + \pi(H) = \mathbb{F}_p^N$, where $\pi(H) = \{\pi(x) : x \in H\}$. Indeed, if $x \in \mathbb{F}_p^N$ is written as $x = w + y$ with $w \in W$ and $y \in H$, then we can also write $x = w - (\pi(y) - y) + \pi(y)$ with $w - (\pi(y) - y) \in W$ and $\pi(y) \in \pi(H)$. Therefore, in order prove Lemma 4.1, it is enough to show the following.

Claim 4.2. There exists $c' > 0$ such that if $M$ is sufficiently large with respect to $p$, then

$$|\pi(H)| \leq 2^{c'(\log r)M}.$$ 

Proof. Clearly, $|\pi(H)| = |\nu(H)|$, so it is enough to show that $|\nu(H)| \leq 2^{c'(\log r)M}$. Let $R_0 = [-r^3, r^3]$, and for $\ell = 1, 2, \ldots$, let

$$R_\ell = [-r^{3 \cdot 2^\ell}, -r^{3 \cdot 2^{\ell-1}} - 1] \cup [r^{3 \cdot 2^{\ell-1}} + 1, r^{3 \cdot 2^\ell}].$$

Then $R_0, R_1, \ldots$ form a partition of the integers. Also, for $b \in \mathbb{F}_p$, let $b^*$ be the unique integer in $[-(p-1)/2, (p-1)/2]$ congruent to $b$ modulo $p$. For $y \in \mathbb{F}_p^M$ and $\ell \in \mathbb{N}$, let $T(\ell, y)$ denote the number of indices $j \in [M]$ such that $y(j)^* \in R_\ell$.

Note that if $x \in \mathbb{F}_p^N$ and $(\nu(x)(j))^* \in R_\ell$ for some $\ell \geq 1$, then at least one of the coordinates $x(i)$ for $i \in I_j$ is not contained in $[-r^{2^{\ell-1}}, r^{2^{\ell-1}}]$, that is, there exists $i \in I_j$ such that $\tau(x(i)) \geq \ell + 2 \log_2 r$. By the definition of $H$, if $x \in H$, then the number of $i \in [N]$ satisfying $\tau(x(i)) \geq \ell + 2 \log_2 r$, and thus the number of $j \in [M]$ satisfying $(\nu(x)(j))^* \in R_\ell$ is at most

$$\sum_{k \geq \ell + 2 \log_2 r} 100(k + 1)^2 2^{-k} N < \frac{c_0 N(\ell + 1)^2 2^{-\ell}}{r} \leq c_0 M(\ell + 1)^22^{-\ell}$$

for some constant $c_0 \geq 1$. Hence, we have

$$T(\ell, \nu(x)) \leq c_0 M(\ell + 1)^22^{-\ell},$$

which also holds for $\ell = 0$. Moreover, if $\ell \geq \log_2 p$, then $T(\ell, \nu(x)) = 0$.

Given nonnegative integers $m_0, m_1, \ldots$ such that $\sum_{\ell \geq 0} m_\ell = M$, the number of vectors $y \in \mathbb{F}_p^M$ satisfying $T(\ell, y) = m_\ell$ is

$$\prod_{\ell \geq 0} |R_\ell|^{m_\ell} \left( M - \sum_{k=0}^{\ell-1} m_k \right) \leq \prod_{\ell \geq 0} |R_\ell|^{m_\ell} \left( \frac{M}{m_\ell} \right) < \prod_{\ell \geq 0} \left( \frac{eM |R_\ell|}{m_\ell} \right)^{m_\ell}.$$
Hence, if $m_\ell$ satisfies the constraint $m_\ell \leq c_0 M (\ell + 1)^2 2^{-\ell}$ for $\ell \in \mathbb{N}$, then the left hand side can be further bounded by
\[
\prod_{\ell \geq 0} \left( 2 c_0 3^2 2^\ell \right) c_0 M (\ell + 1)^2 2^{-\ell} \leq 2^{c_0 M} \sum_{\ell \geq 0} (2 + 3 \log_2 r + 2 \ell) (\ell + 1)^2 2^{-\ell} < 2 c_1 M \log r,
\]
where $c_1 > 0$ is a suitable constant. The number of choices for the nonnegative integers $m_0, m_1, \ldots$ satisfying $\sum_{\ell \geq 0} m_\ell = M$ and $m_\ell = 0$ if $\ell \geq \log_2 p$, is at most $M^{\log_2 p}$, so we get that
\[
|\nu(H)| \leq M^{\log_2 p} 2 c_1 M \log r < 2^{c_1 M \log r},
\]
where the last inequality holds assuming $M$ is sufficiently large with respect to $p$. \hfill \square

This concludes the proof of Lemma 4.1 as well. Now let us turn to the proof of Theorem 1.3, which is an easy deduction.

Proof of Theorem 1.3. Let $v_1, \ldots, v_M \in \mathbb{F}_p^n$ be the normal vectors of $H_1, \ldots, H_M$. There exist positive integers $k_1, \ldots, k_M$ such that $k_i \leq r$ for $i \in [M]$, and there exists an irredundant coset covering of $\mathbb{F}_p^n$ which uses exactly $k_i$ translates of $H_i$ for every $i \in [M]$. Let $V \subset \mathbb{F}_p^n$ be the multiset containing $k_i$ copies of $v_i$. Then $V$ is irredundant, and thus by Lemma 2.2, $W = \ker(V) < \mathbb{F}_p^n$ is versatile. Let $I_1, \ldots, I_M$ be the partition of $V$ in which $I_i$ is the set of copies of $v_i$. Then clearly, $\{w \in \mathbb{F}_p^n : \sum_{i \in I_i} w(v) = 0\} < W$. Therefore, we can apply Lemma 4.1 to conclude that $\dim(W) \geq |V| - \frac{c \log r}{\log p} M$. But then,
\[
\text{codim} \left( \bigcap_{i \in [M]} H_i \right) = \dim(V) = |V| - \dim(\ker(V)) \leq \frac{c \log r}{\log p} M.
\] \hfill \square

Finally, let us prove our result about the choosability version of the Alon-Jaeger-Tarsi conjecture.

Proof of Theorem 1.4. Let $c_0$ be the constant of Theorem 1.3 hidden in the $O(\cdot)$ notation. We show that $\alpha = 1/(2c_0)$ suffices in case $p$ is sufficiently large to satisfy $p^n > 2$.

Let $A \subset \mathbb{F}_p$, be a set of size $r = \lfloor p^n \rfloor \geq 2$, and let $M \in \mathbb{F}_p^n \times n$ be an invertible matrix. Suppose that the statement is false, that is, for every $x \in \mathbb{F}_p^n$, there exists a coordinate of $x$ or $Mx$ in $A$. We use this information to construct a hyperplane covering of $\mathbb{F}_p^n$. Let $e_1, \ldots, e_n$ be the usual unit vectors, and let $v_1, \ldots, v_n$ be the rows of $M$. Then the $2rn$ hyperplanes $H(e_i, -a)$ and $H(v_j, -a)$ for $i, j \in [n]$ and $a \in A$ form a covering of $\mathbb{F}_p^n$. Indeed, if $x \in \mathbb{F}_p^n$, then either $x(i) = a \in A$ for some $i \in [n]$, in which case $x \in H(e_i, -a)$, or $(Mx)(j) = a \in A$ for some $j \in [n]$, in which case $x \in H(v_j, -a)$.

But then we can select a subcollection of these $2rn$ hyperplanes forming an irredundant cover. Let $I \subset [n] \times A$ and $J \subset [n] \times A$ such that the collection of hyperplanes
\[
\mathcal{H} = \{ H(e_i, -a) : (i, a) \in I \} \cup \{ H(v_j, -a) : (j, a) \in J \}
\]
is an irredundant covering. Also, let $I_1 = \{ i \in [n] : \exists a \in A, (i, a) \in I \}$ and $J_1 = \{ j \in [n] : \exists a \in A, (j, a) \in J \}$. Then $\mathcal{H}$ is an irredundant covering which uses at most $r$ translates of the hyperplanes $H(e_i, 0)$ and $H(v_j, 0)$ for $i \in I_1$ and $j \in J_1$. Therefore, by applying Theorem 1.3, we get
\[
\dim(\{e_i : i \in I_1\} \cup \{v_j : j \in J_1\}) < \frac{c_0(|I_1| + |J_1|) \log r}{\log p} < \frac{|I_1| + |J_1|}{2}.
\]
However, note that $\{e_1, \ldots, e_n\}$ and $\{v_1, \ldots, v_n\}$ are both bases, so the left hand side is at least $\max\{|I_1|, |J_1|\}$. This is a contradiction. \hfill \square
5 Concluding remarks

In this paper, we made no serious effort to optimize constants, as we prioritized readability. However, some careful calculations provide fairly reasonable numerical bounds in several theorems, which we discuss in this section. Detailed computations are provided in the Appendix.

- In Theorem 1.1, the upper bound $2^{O(k)}$ can be replaced with $20^k$. See Appendix A.
- In Theorem 1.4, one can take any $\alpha < 1/4$. See Appendix B.
- The first and the second named author [8] proved that the list of primes for which the Alon-Jaeger-Tarsi conjecture holds contains all primes $p \geq 67$, $p \neq 79$. The methods of [8] combined with the new ideas of this paper allow us to add 79 to the list as well. See Appendix C.

Finally, let us remark that we believe our bound on the dimension of versatile subspaces is sharp.

**Conjecture 5.1.** There exists $c > 0$ such that for every prime $p \geq 3$ and sufficiently large $N$, there exists a versatile subspace $V < \mathbb{F}_p^N$ of dimension at most $N(1 - c/\log p)$.

The intuition why this conjecture might be true comes from the observation that if $x \in \mathbb{F}_p^N$ has no zero coordinates and $j \in [N]$, then a random subspace $V < \mathbb{F}_p^N$ of dimension $N(1 - c/\log p)$ (chosen from the uniform distribution) intersects the grid

$$\{y \in \mathbb{F}_p^N : y(j) = x(j) \text{ and } \forall i, y(i) \in \{-x(i), 0, x(i)\}\}$$

with high probability, given $c > 0$ is sufficiently small. If this conjecture is true, it shows that Theorem 1.2 cannot be improved using the approach of this paper.

**Acknowledgements**

J. N. and P. P. P. was supported by the Lendület program of the Hungarian Academy of Sciences (MTA). P. P. P. was also partially supported by the National Research, Development and Innovation Office NKFIH (Grant Nr. K124171 and K129335).
I. T. was supported by the SNSF grant 200021_196965.

**References**

[1] N. Alon, Z. Füredi, Covering the cube with by affine hyperplanes, European J. Combin. 14(2) (1993), 79–83.

[2] N. Alon, N. Linial, and R. Meshulam, Additive bases of vector spaces over prime fields, J. Combin. Theory Ser. A 57 (1991), 203–210.

[3] N. Alon, and M. Tarsi, A nowhere-zero point in linear mappings, Combinatorica 9 (4) (1989), 393–395.

[4] J. Browkin, B. Diviš, and A. Schinzel, Addition of sequences in general fields, Monatsh. Math. 82 (4) (1976), 261–268.

[5] M. DeVos, Matrix choosability, J. Combin. Theory Ser. A 90 (1) (2000), 197–209.
Appendix

Here, we provide some explanation for the numerical values presented in the concluding remarks. We will use the following repeatedly. Let $s_1 \geq s_2 \geq \ldots$ be nonnegative real numbers. We want to maximize

$$\sum_{i \geq 1} x_i \log \left( \frac{1}{x_i} \right)$$

with the restrictions $\sum_{i \geq 1} x_i = 1$ and $0 \leq x_i \leq s_i$ for $i \geq 1$. Using the convexity of the function $f(x) = x \log(1/x)$, the following input maximizes (4). Fix some positive integer $L$, and set $x_i := s_i$ if $i > L$, and let $x_1 = \cdots = x_L := (1 - \sum_{j>L} s_j)/L$. Choose $L$ minimal such that $x_L > x_{L+1}$. Then $(x_i)_{i \geq 1}$ maximizes (4).

Appendix A — Theorem 1.1

In order to get a good constant for Theorem 1.1, we tweak the definition of the key set $H$ in Section 3. For simplicity, we assume that the parameters $p, N$ are sufficiently large. In the proof of Claim 3.4, as $p$ tends to infinity, the stationary distribution $\pi = \pi_p$ converges to the distribution $\pi_0$ defined as $\pi_0(0) = 1/3$, and for $i = 0, 1, \ldots$, $\pi_0(2^i) = \pi_0(-2^i) = 1/(3 \cdot 2^i)$. For $n \in \mathbb{Z}$, define $b_n$ as follows.

- If $|n|$ is not 0 or a power of 2, let $b_n = 0$,
\begin{itemize}
  \item if $n = 2^i$ or $n = -2^i$ for some $i \geq 7$, let $b_n = c \cdot t^i$, where $c = 0.65$, $t = 0.63$,
  \item if $n = 0$ or $n = 2^i$ for some $i \leq 6$, then let $b_n = \infty$.
\end{itemize}

Let $H$ be the set of vectors $v \in \mathbb{Z}^N$ such that the number of coordinates of $v$ equal to $n$ is at most $b_n N$ for every $n \in \mathbb{N}$. With these choices of parameters, $H$ satisfies Claim 3.4, that is, a simple application of Markov's inequality guarantees that with positive probability, a vector whose each coordinate is sampled from $\pi_0$, is contained in $H$. For this, one only needs to ensure that

$$\sum_{n: \pi_0(n) \neq 0} \frac{\pi_0(n)}{b_n} < 1.$$  \hfill (5)

Now let us calculate the size of $H$. Given $x_n \in [0,1]$ for $n \in \mathbb{Z}$ satisfying $x_n N \in \mathbb{N}$ and $\sum_n x_n = 1$, the number of elements of $H$ with exactly $x_n N$ coordinates equal to $n$ is at most

$$\frac{N!}{\prod_{n} (x_n N)!} = \exp \left( (1 + o(1))N \sum_n x_n \log \left( \frac{1}{x_n} \right) \right).$$

Let $B = \sum_{|n| \geq 2^7} b_n = 2ct^7/(1 - t) \approx 0.138$. Then $(1 - o(1))$-proportion of the elements of $H$ have the following distribution of coordinates: for every $n$ which is either $0$ or $|n| = 2^k$ for some $k \leq 6$, the number of coordinates equal to $n$ is $(1 + o(1))N \cdot (1 - B)/13 \approx 0.066 \cdot N$, and for $|n| = 2^k$ with $k \geq 7$, the number of coordinates equal to $n$ is $(1 + o(1))N \cdot b_n$. Therefore, we get that the size of $H$ is roughly $19.168^N \leq 20^N$.

But the size of $H$ directly translates to the upper bound in Theorem 1.1, which then gives $|G : \bigcap_{i=1}^k H_i| \leq 20^k$.

**Appendix B — Theorem 1.4**

Let $\epsilon > 0$ be small, $t = 1/2 + \epsilon$, and $c$ be a parameter specified later. Similarly as before, let $b_n = 0$ if $n$ is not a power of 2, let $b_n = c \cdot t^i$ if $|n| = 2^i$, and let $b_0 = 1$. Let $H$ be the set of vectors $v \in \mathbb{Z}^N$ such that the number of coordinates of $v$ equal to $n$ is at most $b_n N$ for every $n \in \mathbb{N}$. Choose $c$ such that

$$\sum_{n: \pi_0(n) \neq 0} \frac{\pi_0(n)}{b_n} < 1,$$

then $H$ is a set satisfying the requirements of Section 3.1. We want to provide numerical bounds for Claim 4.2, that is, to bound the size of $\nu(H) \subset \mathbb{Z}^M$. Similarly as before, given $x_n \in [0,1]$ for $n \in \mathbb{Z}$ satisfying $x_n M \in \mathbb{N}$ and $\sum_n x_n = 1$, the number of elements of $\nu(H)$ with exactly $x_n M$ coordinates equal to $n$ is at most

$$\exp \left( (1 + o(1))M \sum_n x_n \log \left( \frac{1}{x_n} \right) \right).$$  \hfill (6)

The number of coordinates of $v \in \nu(H)$ in the interval $[r2^\ell - 1, r2^\ell]$ is at most $\sum_{i=\ell}^{\infty} b_2 N \leq cr Mt^\ell/(1 - t)$, therefore we get the constraint

$$\sum_{n=r2^{\ell-1}+1}^{r2^\ell} x_n \leq \frac{cr t^\ell}{1 - t} =: z_\ell,$$  \hfill (7)
and similarly for negative $n$. We want to upper bound

$$
\sum_n x_n \log \left( \frac{1}{x_n} \right)
$$

with respect to these constraints. By the convexity of the function $f(x) = x \log(1/x)$, we can replace constraint (7) with

$$x_n \leq \frac{z}{r2^{t-1}} =: s_n,$$

for $r2^{t-1} + 1 \leq |n| \leq r2^{t}$. Let $L$ be a positive integer, and set $(x_n)_{n \in \mathbb{Z}}$ as follows. If $|n| > L$, then $x_n = s_n$, and $x_n = (1 - \sum_{|i| > L} x_i)/(2L + 1)$ for $|n| \leq L$. If we choose the smallest $L$ for which $x_L \geq x_{L+1}$, $(x_n)_{n \in \mathbb{Z}}$ maximizes (8) under the constraints above. Clearly, we may assume $L = r2^y$ for some positive integer $y$. Here, we have

$$
\sum_{|n| > L} x_n = \sum_{\ell > y} 2s_\ell = \frac{2crty + 1}{(1-t)^2}.
$$

Hence, it is easy to calculate that $y = O(1) + \log r / \log(1/t)$ and $L = r^{1+1/\log_2(1/t) + o(1)}$. Plugging this in (8), we get the upper bound

$$
(\log r) \left( 1 + \frac{1}{\log_2(1/t)} + o(1) \right).
$$

Hence, we deduce $|\nu(H)| \leq r^{M(1+1/\log_2(1/t) + o(1))}$.

But then, we get the following numerical bound for Theorem 1.2:

$$
\text{codim} \left( \bigcap_{i=1}^M H_i \right) \leq M \cdot (\log r) \cdot \left( 1 + 1/\log_2(1/t) + o(1) \right) / \log p.
$$

Using this in the proof of Theorem 1.4, we are looking for the maximal $r$ such that

$$
\frac{(\log r) \cdot (1 + 1/\log_2(1/t) + o(1))}{\log p} \leq \frac{1}{2},
$$

which gives $r \geq p^{1/(2+2/\log_2(1/t) + o(1))}$. Choosing $\epsilon$ sufficiently small, we can choose $\alpha$ to be arbitrarily close to $1/4$.

**Appendix C — Alon Tarsi conjecture for the prime $p = 79$**

In [8] the authors proved the Alon-Jaeger-Tarsi conjecture for primes $67 \leq p \neq 79$. More precisely, the proof works for all primes $p > 3$ for which there exists an arithmetic set $A \subset \mathbb{F}_p$ satisfying $|A|^2 < p - 1$ (we recall that $A$ is arithmetic if each element of $A$ is the middle element of a 3-term arithmetic progression contained in $A$).

For the prime $p = 79$ the minimum size of an arithmetic set is 9, which means that the method introduced in [8] does not work directly. One possible arithmetic set with 9 elements is $A = \{0, 1, 2, 3, 7, 14, 44, 63, 78\} \subset \mathbb{F}_{79}$. Nevertheless, in the following we prove the conjecture for $p = 79$ as well using the method described in the present article.
Assume that the Alon-Jaeger-Tarsi conjecture is not true for \( p = 79 \). From the method of [8] and the current paper, this implies that for some integer \( n \), there is a versatile subspace \( V < \mathbb{F}_{79}^{2n} \) such that \( \dim(V) \leq n \). By taking direct products of many copies, we can again assume that \( n \) is sufficiently large. From the versatile property of the subspace \( V \) we get that \( V + A^{2n} = \mathbb{F}_{79}^{2n} \). This does not give immediately a contradiction, since \( |A^{2n}| = 81^n > 79^n \), however we show in the following that we can replace \( A^{2n} \) with one of its much smaller subsets.

Since \( A \) is an arithmetic set, for each element \( a \in A \) there is a residue \( t(a) \neq 0 \) such that \( a - t(a), a + t(a) \in A \). Indeed, we can take

\[
t(0) = 1, t(1) = 2, t(2) = 1, t(3) = 4, t(7) = 7, t(14) = 30, t(44) = 37, t(63) = 19, t(78) = 15.
\]

For each \( a \in A \), set \( N(a) = \{a - t(a), a + t(a)\} \)

Next, consider an element \( v' \in \mathbb{F}_{79}^{2n} \) and write \( v' = v + x_0 \), where \( v_0 \in V \), \( x_0 \in A^{2n} \). Similarly as in the proof of our main Theorem 1.1, in the \( i \)-th step we use the versatile property of the subspace \( V \) for the coordinate \( i \) (mod \( 2n \)) and the residues \( t(x_j(i)) \), \( 1 \leq j \leq 2n \). We get that there are residues \( \epsilon_j \in \{-1,0,1\}, 1 \leq j \leq 2n \) such that \( \epsilon_j = 1 \) if \( j \equiv i \) (mod \( 2n \)), such that \( d_i = (\epsilon_1 t(x_1(1)), \ldots, \epsilon_{2n} t(x_{2n}(2n))) \in V \). With probability 1/2, we set \( v_{i+1} = v_i + d_i \) and \( x_{i+1} = x_i - d_i \), and with probability 1/2, set \( v_{i+1} = v_i + d_i \) and \( x_{i+1} = x_i - d_i \).

If \( i \) is sufficiently large, we get that for each coordinate \( 1 \leq j \leq 2n \) and element \( a \in A \), the probability \( \mathbb{P}(x_j(i) = a) \) converges to some \( p_a \in [0,1] \) satisfying \( \sum_{a \in A} p_a = 1 \) and

\[
p_a = \frac{\sum_{a' \in A, a \in N(a')} p_{a'}}{2}.
\]

One can calculate that the unique solution of this linear system is

\[
p_0 = \frac{1}{15}, p_1 = \frac{1}{15}, p_2 = \frac{1}{15}, p_3 = \frac{2}{15}, p_7 = \frac{2}{15}, p_{14} = \frac{2}{15}, p_{14} = \frac{2}{15}, p_{63} = \frac{2}{15}, p_{78} = \frac{2}{15}.
\]

This means that if \( i \) is sufficiently large, then for each coordinate \( 1 \leq j \leq 2n \) the probability that \( x_j(i) \in \{0,1,2\} \) is less than \( \frac{1}{9} + \epsilon < 0.21 \). This means that each vector \( v' \in \mathbb{F}_{79}^{2n} \) can be written in a form \( v' = v + x \) such that \( v \in V \), \( x \in A^{2n} \) and the number of coordinates \( 1 \leq j \leq 2n \) such that \( x_j \in \{0,1,2\} \) is less than 0.42\( n \). The number of such vectors \( x \in A^{2n} \) is upper bounded by

\[
2n \cdot 3^{0.42n} \cdot 6^{1.58n} \cdot \left(\frac{2n}{0.42n}\right) \approx 75.211^n < 79^n,
\]

a contradiction. This proves the Alon-Jaeger-Tarsi conjecture for the prime \( p = 79 \).