An uniform version of Dvir and Moran’s theorem

Gábor Hegedűs
Óbuda University
Bécsi út 96/B, Budapest, Hungary, H-1032
hegedus.gabor@uni-obuda.hu

January 8, 2022

Abstract

Dvir and Moran proved the following upper bound for the size of a family $\mathcal{F}$ of subsets of $[n]$ with $\text{Vdim}(\mathcal{F} \Delta \mathcal{F}) \leq d$.

Let $d \leq n$ be integers. Let $\mathcal{F}$ be a family of subsets of $[n]$ with $\text{Vdim}(\mathcal{F} \Delta \mathcal{F}) \leq d$. Then

$$|\mathcal{F}| \leq 2^{\binom{\lfloor d/2 \rfloor}{n}}.$$

Our main result is the following uniform version of Dvir and Moran’s result.

Let $d \leq n$ be integers. Let $\mathcal{F}$ be an uniform family of subsets of $[n]$ with $\text{Vdim}(\mathcal{F} \Delta \mathcal{F}) \leq d$. Then

$$|\mathcal{F}| \leq 2^{\binom{n}{\lfloor d/2 \rfloor}}.$$

Denote by $\mathbf{v}_F \in \{0, 1\}^n$ the characteristic vector of a set $F \subseteq [n]$.

Our proof is based on the following uniform version of Croot-Lev-Pach Lemma:

Let $0 \leq d \leq n$ be integers. Let $\mathcal{H}$ be a $k$-uniform family of subsets of $[n]$. Let $\mathbb{F}$ be a field. Suppose that there exists a polynomial $P(x_1, \ldots, x_n, y_1, \ldots, y_n) \in \mathbb{F}[x_1, \ldots, x_n, y_1, \ldots, y_n]$ with $\deg(P) \leq d$.
such that $P(v_F, v_F) \neq 0$ for each $F \in \mathcal{H}$ and $P(v_F, v_G) = 0$ for each $F \neq G \in \mathcal{H}$. Then

$$|\mathcal{H}| \leq 2 \left( \frac{n}{\lfloor d/2 \rfloor} \right).$$

1 Introduction

Throughout this paper $n$ denotes a positive integer, and $[n]$ stands for the set $\{1, 2, \ldots, n\}$. We denote by $2^n$ the set of all subsets of $[n]$. Subsets of $2^n$ are called set families. Let $\binom{[n]}{m}$ denote the family of all subsets of $[n]$ which have cardinality $m$, and $\binom{[n]}{\leq m}$ of all subsets that have size at most $m$.

A family $\mathcal{F}$ of subsets of $[n]$ is $k$-uniform, if $|F| = k$ for each $F \in \mathcal{F}$.

Let $\mathbb{F}$ be a field. $\mathbb{F}[x_1, \ldots, x_n] = \mathbb{F}[x]$ denotes the ring of polynomials in the variables $x_1, \ldots, x_n$ over $\mathbb{F}$. For a subset $F \subseteq [n]$ we write $x_F = \prod_{j \in F} x_j$. In particular, $x_\emptyset = 1$.

We denote by $v_F \in \{0, 1\}^n$ the characteristic vector of a set $F \subseteq [n]$.

It is a challenging old problem to find strong upper bounds for the size of progression-free subsets in finite Abelian groups. Croot, Lev and Pach achieved recently a breakthrough in this research area and proved a new exponential upper bound for the size of three-term progression-free subsets in the groups $(\mathbb{Z}_4)^n$ (see [4]), where $n \geq 1$ is an arbitrary integer. They based their proof on the following simple statement (see [4] Lemma 1).

Proposition 1.1 Suppose that $n \geq 1$ and $d \geq 0$ are integers, $P$ is a multilinear polynomial in $n$ variables of total degree at most $d$ over a field $\mathbb{F}$, and $A \subseteq \mathbb{F}^n$ is a subset with

$$|A| > 2 \sum_{i=0}^{\lfloor d/2 \rfloor} \binom{n}{i}.$$ 

If $P(a - b) = 0$ for all $a, b \in A$, $a \neq b$, then $P(0) = 0$.

Consider a family $\mathcal{F}$ of subsets of $[n]$. We say that $\mathcal{F}$ shatters $M \subseteq [n]$ if

$$\{F \cap M : F \in \mathcal{F}\} = 2^M.$$ 

Define

$$\text{sh}(\mathcal{F}) = \{M \subseteq [n] : \mathcal{F} \text{ shatters } M\}.$$
We say that a family $\mathcal{F}$ has *VC-dimension* $m$, if $m$ is the maximum of the size of sets shattered by $\mathcal{F}$. We denote by $\text{Vdim}(\mathcal{F})$ the VC-dimension of a family $\mathcal{F}$.

The following result is fundamental in the theory of shattering.

**Theorem** (Sauer[10], Perles, Shelah[11], Vapnik, Chervonenkis[12])

Let $\mathcal{F}$ be a family of subsets of $[n]$ with $\text{Vdim}(\mathcal{F}) \leq d$. Then

$$|\mathcal{F}| \leq \sum_{k=0}^{d} \binom{n}{k}$$

and the upper bound is sharp.

Let $\mathcal{F}$ and $\mathcal{G}$ be families of subsets of $[n]$. We denote by $\mathcal{F} \Delta \mathcal{G}$ the symmetric difference of these families:

$$\mathcal{F} \Delta \mathcal{G} := \{ A \Delta B : A \in \mathcal{F}, B \in \mathcal{G} \}.$$

Dvir and Moran proved an upper bound for the size of a family $\mathcal{F}$ of subsets of $[n]$ with $\text{Vdim}(\mathcal{F} \Delta \mathcal{F}) \leq d$. Their proof based on Proposition 1.1.

**Theorem 1.2** Let $0 \leq d \leq n$ be integers. Let $\mathcal{F}$ be a family of subsets of $[n]$ with $\text{Vdim}(\mathcal{F} \Delta \mathcal{F}) \leq d$. Then

$$|\mathcal{F}| \leq 2 \sum_{k=0}^{\lfloor d/2 \rfloor} \binom{n}{k}.$$

Cambie, Girão and Kang proved the following improved version of Theorem 1.2 in [2].

**Theorem 1.3** Let $d < n$ be positive integers with $d \equiv r \pmod{2}$ for some $r \in \{0, 1\}$. Let $\mathcal{F}$ be a family of subsets of $[n]$ with $\text{Vdim}(\mathcal{F} \Delta \mathcal{F}) \leq d$. Then

$$|\mathcal{F}| \leq 2^r \sum_{k=0}^{\lfloor d/2 \rfloor} \binom{n-r}{k}.$$

Kleitman’s theorem (see [7]) is an immediate consequence of Theorem 1.3.
Corollary 1.4 Let $d < n$ be positive integers with $d \equiv r \pmod{2}$ for some $r \in \{0,1\}$. Let $\mathcal{F}$ be a family of subsets of $[n]$ with $\mathcal{F} \Delta \mathcal{F} \subseteq \binom{[n]}{\leq d}$. Then

$$|\mathcal{F}| \leq 2^r \sum_{k=0}^{\lfloor d/2 \rfloor} \binom{n-r}{k}.$$ 

Our main result is the following uniform version of Theorem 1.2.

Theorem 1.5 Let $d \leq n$ be integers. Let $\mathcal{F}$ be an uniform family of subsets of $[n]$ with $\operatorname{Vdim}(\mathcal{F} \Delta \mathcal{F}) \leq d$. Then

$$|\mathcal{F}| \leq 2^\left( \binom{n}{\lfloor d/2 \rfloor} \right).$$

We prove here a new uniform version of Proposition 1.1. The proof of Theorem 1.3 is based completely on this result.

Theorem 1.6 Let $0 \leq d \leq n$ be integers. Let $\mathcal{H}$ be a $k$-uniform family of subsets of $[n]$. Let $\mathbb{F}$ be a field. Suppose that there exists a polynomial $P(x,y) \in \mathbb{F}[x,y]$ with $\deg(P) \leq d$ (here $x = (x_1,\ldots,x_n), y = (y_1,\ldots,y_n)$) such that $P(v_F,v_F) \neq 0$ for each $F \in \mathcal{H}$ and $P(v_F,v_G) = 0$ for each $F \neq G \in \mathcal{H}$. Then

$$|\mathcal{H}| \leq 2^\left( \binom{n}{\lfloor d/2 \rfloor} \right).$$

In Section 2 we collected the preliminaries about Gröbner basis theory and standard monomials. In Section 3 we present our proofs. In Section 4 we give an interesting conjecture which strengthens our main result.

2 Preliminaries

Define $V(\mathcal{F})$ as the subset $\{v_F : F \in \mathcal{F}\} \subseteq \{0,1\}^n \subseteq \mathbb{F}^n$ for any family of subsets $\mathcal{F} \subseteq \mathcal{P}([n])$.

It is natural to consider the ideal $I(V(\mathcal{F}))$:

$$I(V(\mathcal{F})) := \{f \in \mathbb{F}[x] : f(v) = 0 \text{ whenever } v \in V(\mathcal{F})\}.$$
It is easy to verify that we can identify the algebra $\mathbb{F}[x]/I(V(\mathcal{F}))$ and the algebra of $\mathbb{F}$ valued functions on $V(\mathcal{F})$. Consequently

$$\dim_\mathbb{F} \mathbb{F}[x]/I(V(\mathcal{F})) = |\mathcal{F}|.$$ 

We recall some basic facts about Gröbner basis theory and standard monomials. We refer to [1], [3] for details.

We say that a linear order $\prec$ on the monomials is a term order, if 1 is the minimal element of $\prec$, and $uw \prec vw$ holds for any monomials $u, v, w$ with $u \prec v$. The two most important term orders are the lexicographic order $\prec_l$ and the deglex order $\prec_d$. Recall the definition of the deglex order: we have $u \prec_d v$ iff either $\deg u < \deg v$, or $\deg u = \deg v$, and $u \prec_l v$.

The leading monomial $\text{lm}(f)$ of a nonzero polynomial $f \in \mathbb{F}[x]$ is the $\prec$-largest monomial which appears with nonzero coefficient in $f$.

Let $I$ be an ideal of $\mathbb{F}[x]$. A finite subset $G \subseteq I$ is a Gröbner basis of $I$ if for every $f \in I$ there exists a $g \in G$ such that $\text{lm}(g)$ divides $\text{lm}(f)$. It can be shown that $G$ is actually a basis of $I$, i.e. $G$ generates $I$ as an ideal of $\mathbb{F}[x]$ (cf. [2] Corollary 2.5.6). A well–known fact is (cf. [1] Corollary 1.6.5, Theorem 1.9.1]) that every nonzero ideal $I$ of $\mathbb{F}[x]$ has a Gröbner basis.

A monomial $z \in \mathbb{F}[x]$ is a standard monomial for $I$ if it is not a leading monomial for any $f \in I$. We denote by $\text{sm}(I)$ the set of standard monomials of $I$.

Let $\mathcal{F} \subseteq 2^{[n]}$ be a set family. It is easy to check that the standard monomials of the ideal $I(\mathcal{F}) := I(V(\mathcal{F}))$ are square-free monomials.

It is a fundamental fact that $\text{sm}(I)$ gives a basis of the $\mathbb{F}$-vector-space $\mathbb{F}[x]/I$. This means that every polynomial $g \in \mathbb{F}[x]$ can be uniquely written in the form $h + f$ where $f \in I$ and $h$ is a unique $\mathbb{F}$-linear combination of monomials from $\text{sm}(I)$. Consequently if $g \in \mathbb{F}[x]$ is an arbitrary polynomial and $G$ is a Gröbner basis of $I$, then we can reduce $g$ with $G$ into a linear combination of standard monomials for $I$.

3 Proofs

Let $0 \leq k \leq n/2$, where $k$ and $n$ are integers. Let $\mathcal{M}_{k,n}$ stand for the set of all monomials $x_G$ such that $G = \{s_1 < s_2 < \ldots < s_j\} \subset [n]$ for which $j \leq k$ and $s_i \geq 2i$ holds for every $i$, $1 \leq i \leq j$. We write $\mathcal{M}_{k}$ instead of the more
precise $\mathcal{M}_{k,n}$, if $n$ is clear from the context. It is easy to check that

$$|\mathcal{M}_k| = \binom{n}{k}.$$ 

Let $\mathcal{D}_{k,n}$ denote the set of all sets $H = \{s_1 < s_2 < \ldots < s_j\} \subset [n]$ for which $j \leq k$ and $s_i \geq 2i$ holds for every $i$, $1 \leq i \leq j$.

We described completely the standard monomials of the complete uniform families of all $k$ element subsets of $[n]$ in [6].

**Theorem 3.1** Let $\prec$ an arbitrary term order such that $x_n \prec \ldots \prec x_1$. Let $0 \leq k \leq n$ be integers and define $j := \min(k, n - k)$. Then

$$\text{sm}(V(\binom{[n]}{k})) = \mathcal{M}_{j,n}.$$ 

**Corollary 3.2** Let $0 \leq k \leq n$ be integers and define $j := \min(k, n - k)$. Suppose that $d \leq j$. Then

$$\mathcal{D}_{k,n} \cap \binom{[n]}{\leq d} = \mathcal{D}_{d,n}.$$ 

Let $0 \leq k \leq n$ be arbitrary integers. Define the vector system

$$\mathcal{F}(n,k,2) := V(\binom{[n]}{k}) \times V(\binom{[n]}{k}) \subseteq \{0,1\}^{2n}.$$ 

It is easy to verify the following Corollary from Theorem 3.1.

**Corollary 3.3** Let $\prec$ an arbitrary term order such that $x_n \prec \ldots \prec x_1$. Let $0 \leq k \leq n$ be integers and define $j := \min(k, n - k)$. Then

$$\text{sm}(\mathcal{F}(n,k,2)) = \{x_{M_1} \cdot y_{M_2} : M_1, M_2 \in \mathcal{D}_{j,n}\} \subseteq \mathbb{F}[x,y].$$ 

Mészáros and Rónyai proved the following result in [8] Lemma 1 (see also [9] Theorem 7).

**Theorem 3.4** Let $\prec$ an arbitrary term order such that $x_n \prec \ldots \prec x_1$. Let $\mathcal{F}$ be a family of subsets of $[n]$. Then $\text{sm}(V(\mathcal{F})) \subseteq \{x_U : U \in \text{sh}(\mathcal{F})\}$. 

6
Proof of Theorem 1.6
Consider the matrix $M \in \mathbb{F}^{\mathcal{H} \times \mathcal{H}}$, where $M_{(F,G)} := P(v_F, v_G)$ for each $F, G \in \mathcal{H}$.

It follows from the assumptions that $M$ is a diagonal matrix, where nonzero elements stand in the diagonal, hence

$$\text{rank}(M) = |\mathcal{H}|.$$ 

Let $Q$ denote the reduction of $P$ via the deglex Gröbner basis of $I(F(n, k, 2))$. Then $\deg(Q) \leq \deg(P) \leq d$ and $M_{(F,G)} = Q(v_F, v_G)$ for each $F, G \in \mathcal{H}$.

Let $j := \min(k, n - k)$. It follows from Corollary 3.3 that we can write the polynomial $Q(x, y)$ into the form

$$Q(x, y) = \sum_{M \in D_{j,n}} c_{M_1, M_2} x_{M_1} \cdot y_{M_2} \in \mathbb{F}_2[x, y],$$

where $c_{M_1, M_2} \in \mathbb{F}_2$ for each $M_1, M_2 \in D_{j,n}$. After grouping the terms of the polynomial $Q(x, y)$ we get that

$$Q(x, y) = \sum_{M \in D_{j,n} \cap \{U: |U| \leq \lfloor d/2 \rfloor\}} c_M x_M g_M(y) + \sum_{J \in D_{j,n} \cap \{U: |U| \leq \lfloor d/2 \rfloor\}} d_J y_J h_J(x),$$

where $c_M, d_J \in \mathbb{F}_2$, $h_J(x) \in \mathbb{F}_2[x]$, $g_M(y) \in \mathbb{F}_2[y]$ for each $J, M \in D_{j,n}$.

Then it follows from Corollary 3.2 that

$$Q(x, y) = \sum_{M \in D_{\lfloor d/2 \rfloor, n}} c_M x_M g_M(y) + \sum_{J \in D_{\lfloor d/2 \rfloor, n}} d_J y_J h_J(x),$$

Since

$$|D_{\lfloor d/2 \rfloor, n}| = \binom{n}{\lfloor d/2 \rfloor},$$

hence we get that

$$\text{rank}(M) \leq 2 \binom{n}{\lfloor d/2 \rfloor}.$$ 

It follows from the equality $\text{rank}(M) = |\mathcal{H}|$ that

$$|\mathcal{H}| \leq 2 \binom{n}{\lfloor d/2 \rfloor}.$$
Proof of Theorem 1.5

Let \( \mathbb{F} := GF(2) \). It follows from Theorem 3.4 that
\[
\mathrm{sm}(V(\mathcal{F}\Delta \mathcal{F}), \preceq_d) \subseteq \{x_U : U \in \text{sh}(\mathcal{F}\Delta \mathcal{F})\}.
\]
Since \( \text{Vdim}(\mathcal{F}\Delta \mathcal{F}) \leq d \), hence
\[
\mathrm{sm}(V(\mathcal{F}\Delta \mathcal{F}), \preceq_d) \subseteq \{x_U : |U| \leq d\}.
\]
Let \( \mathcal{G} \) denote a fixed deglex Gröbner basis of \( I(V(\mathcal{F}\Delta \mathcal{F})) \). Denote by \( g : V(\mathcal{F}\Delta \mathcal{F}) \to \mathbb{F} \) the function where \( g(0) = 1 \) and \( g(v_T) = 0 \) for each \( T \in \mathcal{F}\Delta \mathcal{F} \setminus \{\emptyset\} \).

If we reduce \( g \) with the Gröbner basis \( \mathcal{G} \), we get the polynomial \( g' \in \mathbb{F}[x] \). Clearly \( \deg(g') \leq d \), because \( g' \) is a linear combination of deglex standard monomials of \( I(V(\mathcal{F}\Delta \mathcal{F})) \) and \( \mathrm{sm}(V(\mathcal{F}\Delta \mathcal{F}), \preceq_d) \subseteq \{x_U : |U| \leq d\} \). Since \( \mathcal{G} \) is a Gröbner basis of \( I(V(\mathcal{F}\Delta \mathcal{F})) \), hence
\[
g(v_G) = g'(v_G)
\]
for each \( G \in \mathcal{F}\Delta \mathcal{F} \).

Define the polynomial function \( f : V(\mathcal{F}) \times V(\mathcal{F}) \to \mathbb{F} \) by
\[
f(x, y) := g'(x + y).
\]
Then
\[
f(v_F, v_F) = g'(0) = g(0) = 1
\]
for each \( F \in \mathcal{F} \) and
\[
f(v_F, v_G) = g'(v_F + v_G) = g'(v_{F\Delta G}) = g(v_{F\Delta G}) = 0
\]
for each \( F, G \in \mathcal{F} \), where \( F \neq G \).

We can apply Theorem 1.6 with the choices \( \mathcal{H} := \mathcal{F} \) and \( P(x, y) := f(x, y) \). \( \square \)

4 Concluding remarks

We think that the next conjecture is the best form of Theorem 1.5

**Conjecture 1** Let \( d < n \) be positive integers with \( d \equiv r \mod 2 \) for some \( r \in \{0, 1\} \). Let \( \mathcal{F} \) be an uniform family of subsets of \([n]\) with \( \text{Vdim}(\mathcal{F}\Delta \mathcal{F}) \leq d \). Then
\[
|\mathcal{F}| \leq 2^r \left( \binom{n - r}{\lfloor d/2 \rfloor} \right).
\]
References

[1] W. W. Adams and P. Loustaunau, *An Introduction to Gröbner bases*. AMS (1994).

[2] S. Cambie, A. Girão and R. J. Kang, VC dimension and a union theorem for set systems. *Elect. Journal of Comb.*, **26**, 1-8 (2019).

[3] D. Cox, J. Little and D. O'Shea, *Ideals, Varieties, and Algorithms*. (Springer-Verlag, Berlin, Heidelberg, 1992)

[4] E. Croot, V. Lev and P. Pach, Progression-free sets in $\mathbb{Z}_n^4$. *Annals of Math.*, **185**, 331-337 (2017)

[5] Z. Dvir and S. Moran, A Sauer-Shelah-Perles Lemma for Sumsets. *Elect. Journal of Comb.*, **25(4)**, 4-8 (2018).

[6] G. Hegedűs and L. Rónyai, Gröbner bases for complete uniform families, *Journal of Alg. Comb.* **17** (2003) 171–180 .

[7] D. J. Kleitman, On a combinatorial conjecture of Erdős. *Journal of Comb. Theory, A* **1(2)**, 209-214 (1966).

[8] T. Mészáros and L. Rónyai, Some combinatorial applications of Gröbner bases. In: Algebraic Informatics (Winkler, F. ed.), 4th International Conference, CAI 2011, Linz, Proceedings. 65–83, Springer-Verlag, Heidelberg (2011)

[9] S. Moran and C. Rashtchian, Shattered Sets and the Hilbert Function. In 41st International Symposium on Mathematical Foundations of Computer Science (MFCS 2016) (Vol. 58, p. 70). Schloss Dagstuhl–Leibniz-Zentrum für Informatik.

[10] N. Sauer, On the density of families of sets, *J. Combin. Theory A* **13**, 145–147 (1972).

[11] S. Shelah, A combinatorial problem; stability and order for models and theories in infinitary languages, *Pacific Journal of Math.* **41** 247–261 (1972)
[12] V. N. Vapnik, A. Ya. Chervonenkis, On the uniform convergence of relative frequencies of events to their probabilities, *Theory of Probability and Appl. XVI*, 264–280. (1971)