Affine subspaces

Gábor Hegedűs

Abstract

Let W denote the n-dimensional vector space over the finite field $\mathbb{F}_q$. Define

$$\mathcal{T} := \{\underline{x} + S : \ \underline{x} \neq \underline{0} \text{ and } S \text{ is a linear subspace of } W\}$$

as the set of translated affine subspaces of W, which are not linear subspaces. We prove here a Bollobás–type upper bound with respect to the set of translated affine subspaces $\mathcal{T}$. We give also a simple set of pair of translated affine subspaces, which shows that our result is almost sharp.

1 Introduction

First we introduce some notations.

In the following let $q = r^\alpha$ be a fixed prime power, $n \geq 0$ be a nonnegative integer. Let W denote the n-dimensional vector space over the finite field $\mathbb{F}_q$.

Let

$$\mathcal{S} := \{S \subseteq \mathbb{F}_q^n : \ S \text{ is a linear subspace of } W\}$$

denote the set of linear subspaces of the vector space W. Define

$$\mathcal{T} := \{\underline{x} + S : \ \underline{x} \neq \underline{0} \text{ and } S \in \mathcal{S}\}$$

as the set of translated affine subspaces of W, which are not linear subspaces.

Let

$$\mathcal{L} := \{L \in \mathcal{S} : \ \dim L = 1\}$$

denote the set of all *lines* of the vector space W.

B. Bollobás proved in 1966 the following result.

Theorem 1.1 *Let $A_1, \dots, A_m$ and $B_1, \dots, B_m$ be two families of sets such that $A_i \cap B_j = \emptyset$ only if $i = j$. Then*

$$\sum_{i=1}^{m} \frac{1}{\binom{|A_i|+|B_i|}{|A_i|}} \leq 1.$$

In particular if $|A_i| = r$ and $|B_i| = s$ for each $1 \leq i \leq m$, then

$$m \leq \binom{r+s}{r}.$$

The following strengthening of the uniform version of Bollobás's theorem called the *Skew Bollobás's theorem* was proved by L. Lovász.

Theorem 1.2 *If $\mathcal{F} = \{A_1, \dots, A_m\}$ is an r-uniform family and $\mathcal{G} = \{B_1, \dots, B_m\}$ is an s-uniform family such that*

$$(a)\ A_i \cap B_i = \emptyset$$

for each $1 \leq i \leq m$ and

$$(b)\ A_i \cap B_j \neq \emptyset$$

whenever $i < j$ $(1 \leq i, j \leq m)$, then

$$m \leq \binom{r+s}{r}.$$

Lovász also proved the following generalization of Bollobás's theorem for subspaces of a linear space:

Theorem 1.3 *Let $\mathbb{F}$ be an arbitrary field and W be an n-dimensional linear space over the field $\mathbb{F}$.*

Let $U_1, \dots, U_m \in \mathcal{S}$ denote r-dimensional subspaces of W and $V_1, \dots, V_m \in \mathcal{S}$ denote s-dimensional subspaces of W. Assume that

$$(a)\ U_i \cap V_i = \{\underline{0}\}$$

for each $1 \leq i \leq m$ and

$$(b)\ U_i \cap V_j \neq \{\underline{0}\}$$

whenever $i < j$ $(1 \leq i, j \leq m)$. Then

$$m \leq \binom{r+s}{r}.$$

Our main result is the following modification of Lovász's Theorem:

Theorem 1.4 *Let $U_1, \dots, U_m \in \mathcal{T}$ and $V_1, \dots, V_m \in \mathcal{T}$ be translated affine subspaces of an n-dimensional linear space W over the finite field $\mathbb{F}_q$, where $q \neq 2$. Assume that*

$$(a)\ U_i \cap V_i = \emptyset$$

for each $1 \leq i \leq m$ and

$$(b)\ U_i \cap V_j \neq \emptyset,$$

whenever $i < j$ $(1 \leq i, j \leq m)$. Then

$$m \leq \frac{q^n - 1}{q - 1} + 1.$$

In the proof we use the combination of Gröbner basis reduction and the polynomial subspace method.

2 The proof of the main result

2.1 Gröbner bases and standard monomials

We recall now some basic facts concerning Gröbner bases in polynomial rings. A total order $\prec$ on the monomials (words) Mon is a *term order*, if 1 is the minimal element of $\prec$, and $uw \prec vw$ holds for any monomials u, v, w with $u \prec v$. There are many interesting term orders. We define now the lexicographic (lex) and the deglex term orders. Let $u = x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$ and $v = x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}$ be two monomials. Then u is smaller than v with respect to lex ($u \prec_{lex} v$ in notation) iff $i_k < j_k$ holds for the smallest index k such that $i_k \neq j_k$. Similarly, u is smaller than v with respect to deglex ($u \prec_{deg} v$ in notation) iff either $\deg u < \deg v$, or $\deg u = \deg v$ and $u \prec_{lex} v$. Note that we have $x_n \prec x_{n-1} \prec \dots \prec x_1$, for both lex and deglex. The *leading monomial* $\mathrm{lm}(f)$ of a nonzero polynomial $f \in S$ is the largest (with respect to $\prec$) monomial which appears with nonzero coefficient in f when written as a linear combination of different monomials.

Let I be an ideal of S. 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 $\mathrm{lm}(g)$ divides $\mathrm{lm}(f)$. In other words, the leading monomials of the polynomials from G generate the semigroup ideal of monomials $\{\mathrm{lm}(f) : f \in I\}$. Using that $\prec$ is a well founded order, it follows that G is actually a basis of I, i.e., G generates I

as an ideal of S. It is a fundamental fact (cf. [3, Chapter 1, Corollary 3.12] or [1, Corollary 1.6.5, Theorem 1.9.1]) that every nonzero ideal I of S has a Gröbner basis.

A monomial $w \in S$ is called a *standard monomial for* I if it is not a leading monomial of any $f \in I$. Let $\mathrm{Sm}(\prec, I)$ stand for the set of all standard monomials of I with respect to the term-order $\prec$ over $\mathbb{F}$. It follows from the definition and existence of Gröbner bases (see [3, Chapter 1, Section 4]) that for a nonzero ideal I the set $\mathrm{Sm}(\prec, I)$ is a basis of the $\mathbb{F}$-vector-space S/I. More precisely, every $g \in S$ can be written uniquely as $g = h + f$ where $f \in I$ and h is a unique $\mathbb{F}$-linear combination of monomials from $\mathrm{Sm}(\prec, I)$.

2.2 The proof

We need in our proof for the following observation.

Proposition 2.1 *The intersection of a family of affinee subspaces is either empty or equal to a translate of the intersection of their corresponding linear subspaces.*

$\square$

Proof of Theorem 1.4:

Let p be an arbitrary, but fixed prime divisor of $q - 1$. Since $q \neq 2$, hence $p > 1$. We can assign for each subset $F \subseteq \mathbb{F}_q^n$ its characteristic vector $v_F \in \{0,1\}^{q^n} \subseteq \mathbb{F}_p^{q^n}$ such that $v_F(t) = 1$ iff $t \in F$.

Let v_j denote the characteristic vector of V_j.

Consider the polynomials

$$P_i(x_1, \ldots, x_n) := 1 - (\sum_{j=1}^{n} v_{F_i}(j)x_j) \in \mathbb{F}_p[x_1, \ldots, x_n]$$

for each $1 \leq i \leq m$.

Define the following set of polynomials

$$\mathcal{G} := \{x_i^2 - x_i : \ 1 \leq i \leq q^n\} \cup \{x_u - x_v : \ \exists L \in \mathcal{L}, \text{ such that } u, v \in L, u < v\} \tag{1}$$

and let I be the ideal generated by $\mathcal{G}$.

It is easy to verify that these polynomials $\mathcal{G}$ constitute a deglex Gröbner basis of the ideal I. Let $\overline{P_i}$ denote the reduction of P_i via this Gröbner basis $\mathcal{G}$.

Since $\underline{0} \notin U_i, V_i$ for each $1 \le i \le m$, therefore $|L \cap U_i| \le 1$ and $|L \cap V_i| \le 1$ for each line $L \in \mathcal{L}$. Hence $\overline{P_i}(v_j) = P_i(v_j)$ for each $1 \le i, j \le m$.

We claim that the polynomials $\{\overline{P_i} :\ 1 \le i \le m\}$ are linearly independent over $\mathbb{F}_p$. Namely

$$\overline{P_i}(v_i) = P_i(v_i) = 1 - |U_i \cap V_i| = 1$$

by condition (a) and

$$\overline{P_i}(v_j) = P_i(v_j) = 1 - |U_i \cap V_j| = 1 - q^k,$$

where $k \ge 0$, because U_i and V_j were translated affine subspaces and using condition (b). Since

$$q \equiv 1 \pmod{p},$$

thus

$$1 - q^k \equiv 0 \pmod{p}.$$

Therefore the $m \times m$ matrix $P = (\overline{P_i}(v_j))_{1 \le i,j \le m}$ is upper triangular over $\mathbb{F}_p$ and in the diagonal we find nonzero elements. This gives that the matrix is nonsingular and it follows from the Triangular Criterion (Proposition 2.8 in [2]) that the polynomials $\overline{P_1}, \dots, \overline{P_m}$ are linearly independent functions over $\mathbb{F}_p$.

On the other hand, being reduced polynomials with respect to a deglex Gröbner basis of the ideal I, the polynomials $\overline{P_i}$ are linear combinations of standard monomials for I and $\deg(\overline{P_i}) \le \deg(P_i) = 1$, because the deglex reductions can not increase the degree.

Clearly

$$\begin{aligned}\mathrm{Sm}(\prec_{deg}, I) = \{x_1^{u_1} \dots x_n^{u_n} :\ 0 \le u_i \le 1,& \\ \text{and if } \exists L \in \mathcal{L} \text{ s.t. } i, j \in L,\ i < j,\ \text{then } u_j = 0\}.& \quad (2)\end{aligned}$$

We infer that the linearly independent polynomials $\{\overline{P_1}, \dots, \overline{P_m}\}$ are in the $\mathbb{F}_p$-space spanned by

$$\{\underline{x}^u :\ \deg(\underline{x}^u) \le 1 \text{ and } \underline{x}^u \in \mathrm{Sm}(\prec_{deg}, I)\}.$$

Since equation (2) gives that

$$|\{\underline{x}^u : \ \deg(\underline{x}^u) \le 1 \text{ and } \underline{x}^u \in \mathrm{Sm}(\prec_{deg}, I)\}| \le \frac{q^n-1}{q-1} + 1,$$

hence

$$m \le \frac{q^n-1}{q-1} + 1,$$

which was to be proved. $\square$

Proposition 2.2 *Let F_j be arbitrary translated affine subspaces for each $1 \le j \le m$. Let $G_j := F_j + \underline{\alpha_j}$, where $\underline{\alpha_j} \notin F_j$. Then $F_i \cap G_j = \emptyset$ iff $\underline{\alpha_j} \in F_i - F_j$.*

Proof.

First suppose that $\underline{\alpha_j} \in \langle F_i, F_j \rangle$. Then we can write $\underline{\alpha_j}$ into the form

$$\underline{\alpha_j} = \underline{f_i} - \underline{f_j},$$

where $\underline{f_i} \in F_i$ and $\underline{f_j} \in F_j$. Hence $\underline{f_i} = \underline{\alpha_j} + \underline{f_j} \in \underline{\alpha_j} + F_j = G_j$.

Suppose that $F_i \cap G_j \neq \emptyset$. Let $\underline{v} \in F_i \cap G_j$, i.e., $\underline{v} \in F_i$ and $\underline{v} \in \underline{\alpha_j} + F_j$. Then there exists $\underline{f_j} \in F_j$ such that $\underline{v} = \underline{\alpha_j} + \underline{f_j}$. Hence $\underline{\alpha_j} = \underline{v} - \underline{f_j} \in F_i - F_j$. $\square$

In the following we give two system of affine translated subspaces $\{A_1, \dots, A_m\}$ and $\{B_1, \dots, B_m\}$ of an n-dimensional linear space W over the finite field $\mathbb{F}_q$, where $m = \frac{q^n-1}{q-1}$, such that

$$(a) \ A_i \cap B_i = \emptyset$$

for each $1 \le i \le m$ and

$$(b) \ A_i \cap B_j \neq \emptyset,$$

whenever $i < j$ $(1 \le i, j \le m)$.

Let

$$\mathcal{H} = \{H_1, \dots, H_m\}$$

be an enumeration of the set of hyperplanes of the vector space $\mathbb{F}_q^n$. Here $m = \frac{q^n-1}{q-1}$. Define

$$A_i := H_i + \underline{\alpha_i},$$

and

$$B_i := H_i + \underline{\beta_i}$$

where $\underline{\alpha_i} \notin H_i$, $\underline{\beta_i} \notin H_i$ for each $1 \le i \le m$.

It is easy to verify that $A_i, B_i \in \mathcal{T}$ for each $1 \le i \le m$.

Suppose that $\underline{\beta_i} - \underline{\alpha_i} \notin H_i$ for each $1 \le i \le m$, then $A_i \cap B_i = \emptyset$ by the definition of A_i and B_i.

On the other hand, since $\underline{\beta_i} - \underline{\alpha_i} \in H_i - H_j = \mathbb{F}_q^n$, hence Proposition 2.2 gives that $A_i \cap B_j \ne \emptyset$ for each $1 \le i < j \le m$.

References

[1] W. W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases,* American Mathematical Society, 1994.

[2] L. Babai, P. Frankl, *Linear algebra methods in combinatorics,* September 1992.

[3] A. M. Cohen, H. Cuypers and H. Sterk (eds.), *Some Tapas of Computer Algebra,* Springer-Verlag, Berlin, Heidelberg, 1999.

[4] Z. Füredi, Geometric solution of an intersection problem for two hypergraphs, *European J. of Comb.* **5** (1984) 133–136.

[5] P. Pudlák, V. Rödl, A combinatorial approach to complexity, *Combinatorica* **12** (1992), 221–226.

[6] L. Lovász, Flats in matroids and geometric graphs, in: *Combinatorial surveys*, Proc. 6th British Comb. Conf., Egham 1977, Acad. Press, London 1977, 45–86.

[7] Zs. Tuza, Application of Set-Pair Method in Extremal Hypergraph Theory, in "Extremal problems for Finite Sets", *Bolyai Society Mathematical Studies* **3**, János Bolyai Math. Soc., Budapest, 1994, 479–514.