Behrend’s Theorem for Dense Subsets of Finite Vector Spaces

T. C. Brown and J. P. Buhler


1 Introduction

The “combinatorial line conjecture” states that for all \( q \geq 2 \) and \( \varepsilon > 0 \) there exists \( N(q, \varepsilon) \) such that if \( n \geq n(q, \varepsilon) \), \( X \) is a \( q \)-element set, and \( A \) is any subset of \( X^n \) (= cartesian product on \( n \) copies of \( X \)) with more than \( \varepsilon|X^n| \) elements (that is, \( A \) has density greater than \( \varepsilon \)), then \( A \) contains a combinatorial line.

(For a definition of combinatorial line, together with statements and proofs of many results related to the combinatorial line conjecture, including all those results mentioned below, see [5]. Since we are not directly concerned with combinatorial lines in this paper, we do not reproduce the definition here.)

This conjecture (which is a strengthened version of a conjecture of Moser [7]), if true, would bear the same relation to the Hales-Jewett theorem that Szemerédi’s theorem bears to van der Waerden’s theorem. In particular, it would imply Szemerédi’s theorem. The conjecture is known to be true for the case \( q = 2 \) (see [5] or [2]), as was first observed by R. L. Graham. A reward has been offered by Graham for a proof or disproof of the conjecture for the case \( q = 3 \).

A natural weakening of this (apparently very difficult) conjecture is obtained by replacing the integer \( q \) by a prime power \( q \), the \( q \)-element set \( X \) by the \( q \)-element field \( F_q \), the cartesian product \( X^n \) by an \( n \)-dimensional vector space \( V \) over \( F_q \), and “combinatorial line in \( X^n \)” by “affine line in \( V \)”.

(An affine line is any translate of a 1-dimensional vector subspace; the purist will note that we only use the structure of \( V \) as an affine space.)

We thus obtain the “affine line conjecture:" For every prime power \( q \) and \( \varepsilon > 0 \), there exists \( n(q, \varepsilon) \) such that if \( n \geq n(q, \varepsilon) \), \( V \) is an \( n \)-dimensional vector space over the \( q \)-element field, and \( A \) is any subset of \( V \) with more than \( \varepsilon|V| \) elements (that is, \( A \) has density greater than \( \varepsilon \)), then \( A \) contains an affine line.

The affine line conjecture is known to be true for the cases \( q = 2 \) (trivial) and \( q = 3 \) ( [3]). In [4] it is shown that if the affine line conjecture is true for a given fixed value of \( q \), then it remains true for this value of \( q \) when “affine line” is replaced by “\( k \)-dimensional affine subspace”, for any \( k \), and similarly for the combinatorial line conjecture.

Szemerédi’s theorem [9] states that for each \( k \) and \( \varepsilon > 0 \), there exists \( n \) such that if \( A \) is any subset of \( \{1, 2, \ldots, n\} \) with more than \( \varepsilon n \) elements (that is, \( A \) has density greater than \( \varepsilon \)), then \( A \) contains a \( k \)-term arithmetic progression. Some 37 years prior to the proof of Szemerédi’s theorem, Felix Behrend [1]
proved the following result: If Szemerédi’s theorem is false then there exist triples \((k, n, A)\) such that \(A\) is a subset of \(\{1, 2, \ldots, n\}\) which contains no \(k\)-term arithmetic progression, \(n\) is arbitrarily large, and the density of \(A\) in \(\{1, 2, \ldots, n\}\) \((= |A|/n)\) is arbitrarily close to 1.

In [2], the exact analogue of Behrend’s result was established in the context of the combinatorial line conjecture: If the combinatorial line conjecture is false then there exist triples \((X, n, A)\) such that \(X\) is a finite set, \(A\) is a subset of \(X^n\) which contains no combinatorial line, \(n\) is arbitrarily large, and then density of \(A\) in \(X^n\) \((= |A|/|X^n|)\) is arbitrarily close to 1.

In the present paper we show that the exact analogue of Behrend’s result is true in the context of the affine line conjecture: If the affine line conjecture is false then there exist triples \((F, n, A)\) such that \(F\) is a finite field, \(A\) is a subset of \(F^n\) (the \(n\)-dimensional vector space over \(F\)) which contains no affine line, \(n\) is arbitrarily large, and then density of \(A\) in \(F^n\) \((= |A|/|F^n|)\) is arbitrarily close to 1.

The proof is somewhat technical, and the exact result which we prove is following. Suppose that the affine line conjecture fails for the finite field \(F\). (That is, let \(|F| = q\) and suppose that \(n(q, \varepsilon)\) does not exist for some \(\varepsilon > 0\).) Then for every \(\eta < 1\) and every \(n_0\) there is a subset \(A\) of a finite-dimensional vector space \(V\) over a finite extension \(F^*\) of \(F\), where \(\dim_{F^*} V \geq n_0\), such that \(A\) contains no affine line and the density of \(A\) in \(V\) \((= |A|/|V|)\) is greater than \(\eta\).

The proof is basically a modification of the argument in [2], which in turn followed the lines of the classical paper by Behrend [1].

## 2 Notation, definitions, and statement of the main theorem

Throughout, \(F_q\) denotes the \(q\)-element field.

**Definition 1.** For each prime power \(q\) and \(\varepsilon > 0\), \(n(q, \varepsilon)\) denotes the smallest integer (if one exists) such that if \(V\) is a finite-dimensional vector space over \(F_q\), \(\dim(V) \geq n(q, \varepsilon)\), \(A \subset V\), \(|A| > \varepsilon|V|\), then \(A\) contains an affine line.

For a fixed prime power \(q\), consider the infinite array

\[
m(q) = (d(n, k)) \quad (n \geq 1, k \geq 1)
\]

where the rows are indexed by \(n\) and the columns are indexed by \(k\), and where \(d(n, k)\) is defined as follows. Let \(V\) be an \(n\)-dimensional vector space over \(F_q\), and let \(A\) be a subset of \(V\) that has maximum cardinality subject to the condition that \(A\) contains no affine line. Then

\[
d(n, k) = |A|/|V|.
\]

In other words, \(d(n, k)\) is the smallest real number with the following property. If \(B\) is any subset of \(V\) (\(V\) as above) with \(|B| > d(n, k)|V|\), then \(B\) contains an affine line.

**Remark.** It follows directly from the preceding two sentences and the definition of \(n(q, \varepsilon)\) that for all \(n, k\),

\[
n \geq n(q^k, \varepsilon) \quad \text{if and only if} \quad d(n, k) \leq \varepsilon.
\]
We shall see below that each column of the array $M(q)$ decreases. We define, for each $k \geq 1$,

$$\gamma(k) = \lim_{n \to \infty} d(n,k),$$

so that

$$d(1,k) \geq \cdots \geq d(n,k) \geq \cdots \geq \gamma(k).$$

We shall also see that for each row of $M(q)$,

$$d(n,1) \leq d(n,2) \leq \cdots \leq d(n,2^l) \leq \cdots \leq 1,$$

so that

$$0 \leq \gamma(1) \leq \cdots \leq \gamma(2^l k) \leq \cdots \leq \Gamma(q),$$

where by definition

$$\Gamma(q) = \lim_{l \to \infty} \gamma(2^l).$$

**Theorem.** $\Gamma(q) = 0$ or $\Gamma(q) = 1$.

**Corollary.** Suppose the affine line conjecture is false. In particular, suppose that $n(q, \varepsilon)$ does not exist. Let $\eta < 1$ be given. Then there exists an integer $k$ and a subset $A$ of a finite-dimensional vector space $V$ (of arbitrarily large dimension) over $\mathbb{F}_q$, such that $A$ contains no affine line and $A$ has density greater than $\eta$.

**Proof of Corollary.** We prove the contrapositive. We are assuming that (as is shown in Lemma 1 below) $d(n,k)$ decreases to $\gamma(k)$ and that $\gamma(2^l)$ increases to $\Gamma(q)$.

Now let $q$ and $\eta < 1$ be given, and suppose that for each $k \geq 1$, if $A$ is a subset of a vector space $V$ over $\mathbb{F}_q$ with density greater than $\eta$, and $\dim V$ is sufficiently large, then $A$ must contain an affine line. In other words, we are assuming that $n(q^k, \eta)$ exists for all $k \geq 1$. We need to show that $n(q, \varepsilon)$ exists for all $\varepsilon > 0$.

Construct the array $M(q)$ as above, and consider the entries $d(n,k)$ in the $k$th column of $M(q)$. Since $n(q^k, \eta)$ exists then by the Remark above

$$d(n,k) \leq \eta \quad \text{for all } n \geq n(q^k, \eta).$$

Since $d(n,k)$ decreases to $\gamma(k)$, it follows that $\gamma(k) \leq \eta$, for each $k \geq 1$. In particular, $\gamma(2^l) \leq \eta$ for each $l$; since $\gamma(2^l)$ increases to $\gamma(q)$, it follows that $\Gamma(q) \leq \eta < 1$. By the theorem, we must have $\Gamma(q) = 0$ and hence $\gamma(1) = 0$.

Now let $\varepsilon > 0$ be given. Since $d(n,1)$ decreases to $\gamma(1) = 0$, $d(n,1) < \varepsilon$ for sufficiently large $n$, say $d(n_0,1) < \varepsilon$. Then using the Remark once more, we obtain $n_0 \geq n(q, \varepsilon)$. Thus, $n(q, \varepsilon)$ exists.

**3 Proof of the main theorem**

**Lemma 1.** Fix $q$, and let the numbers $d(n,k)$ be defined as above. Then

$$d(1,k) \geq \cdots \geq d(n,k) \geq d(n+1,k) \geq \cdots$$
and
\[ d(n, 1) \leq \cdots \leq d(n, 2^l) \leq d(n, 2^{l+1}) \leq \cdots. \]

**Proof.** For the first part, let
\[ \dim_{\mathbb{F}_{q^k}} V = n + 1 \]
and let \( V_0 \) be an \( n \)-dimensional subspace of \( V \). Let
\[ V = \bigcup \{ V_\alpha : \alpha \in \mathbb{F}_{q^k} \}, \]
where the \( V_\alpha \) are cosets (translates) of \( V_0 \). Let \( A \) be a subset of \( V \) which has maximum cardinality subject to the condition that \( A \) contains no affine line. Then \( A \cap V_\alpha \) contains no affine line for each \( \alpha \), hence
\[ d(n + 1, k) \cdot (q^k)^{n+1} = |A| = \sum |A \cap V_\alpha| \leq q^k \cdot d(n, k) \cdot (q^k)^n. \]

For the second part, let \( F = \mathbb{F}_{q^l} \) and let \( F' = F(\beta) \), where \( \beta \) has degree 2 over \( F \). Let
\[ V = \{ (x_1, \ldots, x_n) : x_i \in F \}, \]
\[ V' = \{ (x_1 + y_1 \beta, \ldots, x_n + y_n \beta) : x_i, y_i \in F \}, \]
so that \( V \subset V' \).

Let \( A \) be an affine-line-free subset of \( V \) with
\[ |A| = d(n, 2^l)|V|, \]
and let \( A' = A + \beta V \). Then \( A' \) is a subset of \( V' \), and \( A' \) contains no affine line. For if \( u_0, v_0, u_1, v_1 \in V \) and
\[ (u_0 + v_0 \beta) + F'(u_1 + v_1 \beta) \subset A', \]
then
\[ u_0 + Fu_1 \subset A. \]
If \( u_1 = 0 \), we use
\[ \beta^2 = x_1 + y_1 \beta, \quad x_1, y_1 \in F, x_1 \neq 0; \]
then \( A' \) contains
\[ (u_0 + v_0 \beta) + F(\beta(u_1 + v_1 \beta) = (u_0 + v_0 \beta) + F(u_1 \beta + v_1 x_1 + v_1 y_1 \beta). \]

So \( A \) contains \( u_0 + Fv_1 \). \[ \square \]

We now fix some further notation which will be used in the remainder of the proof.

**Definition 2.** For any prime power \( q \), \( V(q) = \{ (x_1, x_2, \ldots) : x \in \mathbb{F}_q \} \) and \( x_i = 0 \) for all but finitely many \( i \), and
\[ V(q)(m) = \{ (x_1, x_2, \ldots) \in V(q) : x_j = 0, j > m \}. \]
For any subset $S$ of $V(q)$, 

$$S(m) = S \cap V(q)(m) \quad \text{and} \quad \bar{d}(S) = \limsup_{m \to \infty} |S(m)| \cdot q^{-m}.$$ 

**Lemma 2.** If $S \subset V(q^k)$ and $\bar{d}(S) > \gamma(k)$ (where $\gamma(k)$ is defined in terms of the array $M(q))m$ then $S$ contains an affine line. (That is, $S(m)$ contains an affine line for some $m$.)

**Proof.** Choose $\epsilon > 0$ so that 

$$\gamma(k) + \epsilon < |S(m)| \cdot q^{-km}$$

for infinitely many $m$. Next, choose $n$ so that 

$$d(n,k) < \gamma(k) + \epsilon.$$ 

Finally, choose $m$ so that simultaneously 

$$\gamma(k) + \epsilon < |S(m)| \cdot q^{-km} \quad \text{and} \quad n < m - n.$$ 

Assume that $S$ contains no affine line. Then for each $x \in V(q^k)(n)$, $S(m)$ can contain at most $d(m-n,k) \cdot (q^k)^{m-n}$ elements whose first $n$ coordinates agree with the first $n$ coordinates of $x$. Hence 

$$|S(m)| \leq (q^k)^n \cdot d(m-n,k) \cdot (q^k)^{m-n}.$$ 

Since $d(m-n,k) \leq d(n,k) < \gamma(k) + \epsilon$, this gives 

$$\gamma(k) + \epsilon < |S(m)| q^{-km} < \gamma(k) + \epsilon. \quad \square$$

**Lemma 3.** For each $t \geq 1$, if $S \subset V(q^k)$ and $\bar{d}(S) > \gamma(k t)$ (where $\gamma(k t)$ is defined in terms of the array $M(q)$), then $S$ contains a $t$-dimensional affine subspace.

**Proof.** Identify $\mathbb{F}_{q^t}$ with $\{ (x_1, \ldots, x_t) : x_j \in \mathbb{F}_q \}$, so that 

$$V(q^k)^t = \{ (x_1, \ldots, x_t) : x_j \in \mathbb{F}_{q^k} \}.$$ 

Let $S \subset V(q^k), \bar{d}(S) > \gamma(k t)$. Choose $\epsilon > 0$ so that 

$$|S(m)| \cdot q^{-km} > \gamma(k t) + \epsilon$$

for infinitely many $m$. From amongst these $m$, choose a subsequence $m_0 < m_1 < m_2 < \cdots$ such that all the $m_i$'s are congruent modulo $t$.

Let $\pi : S \mapsto V(q^k)$ be the mapping which shifts an element of $S$ “$m_0$ places to the left,” i.e., 

$$\pi(x_1, \ldots, x_{m_0}, x_{m_0+1}, \ldots) = (x_{m_0+1}, \ldots).$$

For any $T \subset S$, let $T'$ denote $\pi(T)$.
For each $x = (x_1, \ldots, x_{m_0}, 0, \ldots) \in V(q^2)(m_0)$, let

$$S_x = \{y = (y_1, \ldots) \in S : y_i = x_i, 1 \leq i \leq m_0\}.$$ 

Then $S$ is the disjoint union

$$S = \bigcup \{S_x : x \in V(q^2)(m_0)\}.$$ 

Therefore for each $i \geq 1$,

$$\sum_x |S_x(m_i)| = |S(m_i)| > d^{km_i}(\gamma(kt) + \varepsilon).$$

Hence for some $x_i \in V(q^2)(m_0)$,

$$|S'_{x_i}(m_i - m_0)| = |S_{x_i}(m_i)| \geq q^{-km_0}S(m_i)|$$

$$> q^{km_i - m_0}(\gamma(kt) + \varepsilon).$$

Since each $x_i$ comes from the finite set $V(q^2)(m_0)$, there is an infinite subsequence $\{m_j\}$ of $\{m_i\}$ on which $x_i$ is constant, say $x_{i_1} = x_{i_2} = \cdots = x_0$. Set

$$n_j = m_j - m_0, \quad j \geq 1.$$ 

Then each $n_j$ is a multiple of $t$, say

$$n_j = tb_j \quad \text{and} \quad |S'_{x_{i_0}}(n_j)| > q^{km_j}(\gamma(kt) + \varepsilon), \quad j \geq 1.$$ 

We now inject $S_{x_{i_0}}$ into $V(q^{kt})$ by insertion of parentheses, that is, we define $g : S_{x_{i_0}} \mapsto V(q^{kt})$ by

$$g(x_1, \ldots) = ((x_1, \ldots, x_t), (x_{t+1}, \ldots, x_{2t}), \ldots).$$

Then for each $j \geq 1$,

$$|g(S'_{x_{i_0}}(b_j))| = |S'_{x_{i_0}}(tb_j)| = |S'_{x_{i_0}}(n_j)| > (q^{kt})^{b_j}(\gamma(kt) + \varepsilon).$$

This means that in $V(q^{kt})$,

$$\tilde{d}(g(S'_{x_{i_0}})) > \gamma(kt).$$

Here, $\gamma(kt)$ is the limit down the $(kt)$th column of the array $M(q)$, which is identical with the $k$th column of the array $M(q')$. Thus

$$g(S_{x_{i_0}}) \subset V((q^*)^{kt})$$

and

$$\tilde{d}(g(S'_{x_{i_0}})) > \gamma(k)$$

(where $\gamma(k)$ is defined in terms of the array $M(q')$). Hence by Lemma 2 $g(S'_{x_{i_0}})$ contains an affine line. This affine line (the underlying field is $\mathbb{F}_{q^2}$) is easily seen to be the image under $g$ of a $t$-dimensional affine subspace of $S'_{x_{i_0}}$ (where the underlying field if $\mathbb{F}_{q^t}$). From the definition of $S'_{x_{i_0}}$ it follows that $S$
Lemma 4. There exists $S \subset V(q^k)$ such that $\bar{d}(S) = \gamma(k)$ (where $\gamma(k)$ is defined in terms of the array $M(q)$) and such that $S$ contains no affine line.

Proof. Choose $0 = n_0 < n_1 < \cdots$ so that $n_i - n_{i-1} \to \infty$ as $i \to \infty$. For $i \geq 1$, let $A_i \subset V(q^k)(n_i)$ be such that $A_i$ contains no affine line,

$$|A_i| = a^{kn_i}d(n_i, k) \quad \text{and} \quad 0 \notin A_i.$$  

(If $L$ is some fixed affine line $V(q^2)(n_i)$ and $A \subset V(q^2)(n_i)$ contains no affine line, then for some $a \in L$, $a + A$ does not contain 0.) Let

$$B_i = A_i - V(q^k)(n_{i-1}) \quad \text{and} \quad S = \bigcup B_i, \quad i \geq 1.$$  

Then

$$|S(n_i)| \geq |B_i| \geq |A_i| - q^{kn_i}d(n_i, k) = q^{kn_i}d(n_i, k) - (q^k)^{n_i-n_{i-1}},$$  

hence

$$\bar{d}(S) \geq \gamma(k) = \lim_{i \to \infty} d(n_i, k).$$  

The sets $B_i$ are pairwise disjoint, and if $x = (x_1, \ldots) \in S$ and $j$ is the largest index with $x_j \neq 0$ then $x \in B_i$, where $n_{i-1} < j \leq n_i$.

Suppose that $S$ contains the affine line $u_1, \ldots, u_q$. Choose $i_0$ minimal so that $u_1, \ldots, u_q \in B_1 \cup \cdots \cup B_{i_0}$. Then there are $u_s$ and $j$, $n_{i_0-1} < j \leq n_{i_0}$, such that the $j$th coordinate of $u_s$ is not zero. Since the $j$th coordinates of $u_1, \ldots, u_q$ are either constant or are some permutation of $\mathbb{F}_{q^k}$ at least $q^k - 1$ of $u_1, \ldots, u_q$ are contained in $B_{i_0}$. Suppose $u_1 \notin B_{i_0}$. Let $j$ be the largest index such that the $j$th coordinate of $u_1$ is not zero. ($j$ exists since $u_1 \neq 0$.) Then $j < n_{i_0-1}$, and hence the $j$th coordinates of $u_2, \ldots, u_q$ are all zero. But since $u_1, \ldots, u_q$ are an affine line, then the $j$th coordinates are either constant or are a permutation of $\mathbb{F}_{q^k}$.

Thus we have arrived at a contradiction (except in the case $q^k = 2$) and therefore $S$ contains no affine line. (When $q^k = 2$, then $\gamma(1) = 0$. Any singleton set $S = \{x\} \subset V(2)$ has $\bar{d}(S) = 0 = \gamma(1)$, and $S$ contains no affine line.) Since $\bar{d}(S) \geq \gamma(k)$, Lemma 2 gives $\bar{d}(S) = \gamma(k)$. \hfill \Box

We now have necessary machinery to prove the main theorem. Recall that for a prime power $q, M(q)$ is the array

$$((d(n, k)), \quad \gamma(2^l) = \lim_{n \to \infty} d(n, 2^l), \quad \Gamma(q) = \lim_{l \to \infty} \gamma(2^l)).$$

Theorem. For every prime power $q$, $\Gamma(q) = 0$ or $\Gamma(q) = 1$.

Proof. Fix $q$, and assume that $0 < \Gamma(q) < 1$. Choose $l$ so that

$$0 < \gamma(2^l). \quad (1)$$

Using Lemma 4, choose $S \subset V(q^{2^l})$ so that

$$\bar{d}(S) = \gamma(2^l) \quad (2)$$

7
Choose $\varepsilon < 0$ so that
\[
\Gamma(q) < \frac{\gamma(2^l) - \varepsilon}{\gamma(2^l) + \varepsilon}.
\]
Choose $n$ so that
\[
\left\{ A \subset V(q^k)(n) \mid |A| > (\gamma(2^l) + \varepsilon)q^{kn} \right\} \Rightarrow \left\{ A \text{ contains an affine line} \right\}.
\]
Choose $t$ (using the extended Hales-Jewett theorem; see [5] or [8]) so that $t$ is a power of 2 and
\[
\left\{ T \text{ is a } t\text{-dimensional affine subspace} \mid \text{and } T = T_1 \cup \cdots \cup T_s, \text{ where } s = 2^{t^n-1} \right\} \Rightarrow \left\{ \text{some } T_j \text{ contains an affine line} \right\}.
\]
Set
\[
V' = V(q^k) - V(q^k)(n), \quad B_v = (v + V(q^k)(n)) \cap S, \quad v \in V'.
\]
Partition $V'$ into $2^{t^n}$ classes $C_\sigma$ as follows.
\[
C_\sigma = \{ v \in V' : B_v = v + \sigma \}, \quad \sigma \subset V(q^k)(n).
\]
(Note that $C_\sigma = \{ v \in V' : B_v = \emptyset \}.$)

Let
\[
\bar{d}_\nu(C) = \limsup_{m \to \infty} (q^{-k})^{m-n} |C \cap V'(m)|.
\]

Since
\[
|C \cap V'(m)| < \left( \bar{d}_\nu(C) + \varepsilon \right) q^{k(m-n)}
\]
for all but finitely many $m$, and since
\[
|S(m)| > (\gamma(2^l) - \varepsilon)q^{-km}
\]
for infinitely many $m$ (by (2)), we can choose $m$ so that $n < m$ and
\[
(\gamma(2^l) - \varepsilon)q^{km} < |S(m)|
\]
for infinitely many $m$ (by (2)), we can choose $m$ so that $n < m$ and
\[
|C \cap V'(m)| < \left( \bar{d}_\nu(C) + \varepsilon \right) q^{k(m-n)}.
\]

Using (7), (3), and (5) we get
\[
|B_v| \leq (\gamma(2^l) + \varepsilon)q^{kn}, \quad v \in V'.
\]

Note that $m > n$ and
\[
V(q^k)(m) = \bigcup \{ v + V(q^k)(n) : v \in V'(m) \},
\]
so that

\[ V(q^k)(m) \cap S = \bigcup \{ (v + V(q^k)(n) \cap S : v \in V'(m) \} \]

\[ = \bigcup \{ B_v : v \in V'(m) \text{ and } B_v \neq \emptyset \} \]

\[ = \bigcup \{ B_v : v \in V'(m) \cap C \}. \]

That is,

\[ S(m) = \bigcup \{ B_v : v \in V'(m) \cap C \}. \quad (13) \]

Now using (10), (13), (12), (11) we get

\[ (\gamma(2^l) - \varepsilon)q^{kn} < |S(m)| < (\gamma(2^l) + \varepsilon)q^{kn}(d_{\nu}(C) + \varepsilon)q^{k(m-n)}, \]

or

\[ \frac{\gamma(2^l) - \varepsilon}{\gamma(2^l) - \varepsilon} - \varepsilon < d_{\nu}(C). \]

Using (4), this gives

\[ \Gamma(q) < d_{\nu}(C). \quad (14) \]

The integer \( t \) was chosen to be a power of 2, say \( t = 2^b \), and to satisfy (6). Since

\[ \gamma(2^l t) = \gamma(2^{l+b}) \leq \Gamma(q) < d_{\nu}(C), \]

it follows from Lemma 3 that \( C \) contains a \( t \)-dimensional affine subspace \( T \). We partition the elements of \( T \) into \( 2^{(n-1)} \) classes \( C_{\sigma} \cap T, \sigma \neq \phi \). By (6), some \( C_{\sigma_0} \cap T \), and hence some \( C_{\sigma_0} \), contains an affine line \( u_1, \ldots, u_q \). Using (8) and (7), \( u_1 \in C_{\sigma_0} \) implies

\[ u_1 + \sigma_0 = B_{u_1} \cap S. \]

Similarly,

\[ u_i + \sigma_0 = B_{u_i} \cap S, \quad 1 \leq i \leq q^k. \quad (15) \]

In particular, taking any element \( v_0 \in \sigma_0 \) (\( \sigma_0 \neq \phi \)), \( S \) contains the affine line

\[ u_1 + v_0, \ldots, u_q + v_0, \]

which contradicts (3).

This contradiction shows that \( 0 < \Gamma(q) < 1 \) is impossible, and complete the proof. \( \square \)

References


