A strengthened inequality of Alon-Babai-Suzuki’s conjecture on set systems with restricted intersections modulo $p$

Wang Xin$^a$, Hengjia Wei$^b$ and Gennian Ge$^{b,c,*}$

$^a$ School of Mathematical Sciences, Zhejiang University, Hangzhou 310027, Zhejiang, China
$^b$ School of Mathematical Sciences, Capital Normal University, Beijing, 100048, China
$^c$ Beijing Center for Mathematics and Information Interdisciplinary Sciences, Beijing, 100048, China

Abstract

Let $K = \{k_1, k_2, \ldots, k_r\}$ and $L = \{l_1, l_2, \ldots, l_s\}$ be disjoint subsets of $\{0, 1, \ldots, p-1\}$, where $p$ is a prime and $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ be a family of subsets of $[n]$ such that $|A_i| \pmod{p} \in K$ for all $A_i \in \mathcal{A}$ and $|A_i \cap A_j| \pmod{p} \in L$ for $i \neq j$. In 1991, Alon, Babai and Suzuki conjectured that if $n \geq s + \max_{1 \leq i \leq r} k_i$, then $|\mathcal{A}| \leq \binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{s-2r+1}$. In 2000, Qian and Ray-Chaudhuri proved the conjecture under the condition $n \geq 2s - r$. In 2015, Hwang and Kim verified the conjecture of Alon, Babai and Suzuki.

In this paper, we will prove that if $n \geq 2s - 2r + 1$ or $n \geq s + \max_{1 \leq i \leq r} k_i$, then

$$|\mathcal{A}| \leq \binom{n-1}{s} + \binom{n-1}{s-1} + \cdots + \binom{n-1}{s-2r+1}.$$

This result strengthens the upper bound of Alon, Babai and Suzuki’s conjecture when $n \geq 2s - 2$.

1 Introduction

A family $\mathcal{A}$ of subsets of $[n]$ is called intersecting if every pair of distinct subsets $A_i, A_j \in \mathcal{A}$ have a nonempty intersection. Let $L$ be a set of $s$ nonnegative integers. A family $\mathcal{A}$ of subsets of $[n]$ is $L$-intersecting if $|A_i \cap A_j| \in L$ for every pair of distinct subsets $A_i, A_j \in \mathcal{A}$. A family $\mathcal{A}$ is $k$-uniform if it is a collection of $k$-subsets of $[n]$. Thus, a $k$-uniform intersecting family is $L$-intersecting for $L = \{1, 2, \ldots, k-1\}$.

The following is an intersection theorem of de Bruijn and Erdős [4].

**Theorem 1.1** (de Bruijn and Erdős, 1948 [4]). **If $\mathcal{A}$ is a family of subsets of $[n]$ satisfying $|A_i \cap A_j| = 1$ for every pair of distinct subsets $A_i, A_j \in \mathcal{A}$, then $|\mathcal{A}| \leq n$.**

A year later, Bose [2] obtained the following more general intersection theorem which requires the intersections to have exactly $\lambda$ elements.

**Theorem 1.2** (Bose, 1949 [2]). **If $\mathcal{A}$ is a family of subsets of $[n]$ satisfying $|A_i \cap A_j| = \lambda$ for every pair of distinct subsets $A_i, A_j \in \mathcal{A}$, then $|\mathcal{A}| \leq n$.**

$^*$Corresponding author. Email address: 11235062@zju.edu.cn (X. Wang), ven0505@163.com (H. Wei), gnge@zju.edu.cn (G. Ge).
In 1961, Erdős, Ko and Rado [5] proved the following classical result on \(k\)-uniform intersecting families.

**Theorem 1.3** (Erdős, Ko and Rado, 1961 [5]). Let \(n \geq 2k\) and let \(A\) be a \(k\)-uniform intersecting family of subsets of \([n]\). Then \(|A| \leq \binom{n-1}{k-1}\) with equality only when \(A\) consists of all \(k\)-subsets containing a common element.

In 1975, Ray-Chaudhuri and Wilson [11] made a major progress by deriving the following upper bound for a \(k\)-uniform \(L\)-intersecting family.

**Theorem 1.4** (Ray-Chaudhuri and Wilson, 1975 [11]). If \(A\) is a \(k\)-uniform \(L\)-intersecting family of subsets of \([n]\), then \(|A| \leq \binom{n}{k}\).

In terms of parameters \(n\) and \(s\), this inequality is best possible, as shown by the set of all \(s\)-subsets of \([n]\) with \(L = \{0, 1, \ldots, s-1\}.

In 1981, Frankl and Wilson [6] obtained the following celebrated theorem which extends Theorem 1.3 by allowing different subset sizes.

**Theorem 1.5** (Frankl and Wilson, 1981 [6]). If \(A\) is an \(L\)-intersecting family of subsets of \([n]\), then \(|A| \leq \binom{n}{k} + \binom{s-1}{k-1} + \cdots + \binom{0}{0}\).

The upper bound in Theorem 1.5 is best possible, as demonstrated by the set of all subsets of size at most \(s\) of \([n]\).

In the same paper, a modular version of Theorem 1.4 was also proved.

**Theorem 1.6** (Frankl and Wilson, 1981 [6]). If \(A\) is a \(k\)-uniform family of subsets of \([n]\) such that \(k \pmod{p} \not\in L\) and \(|A_i \cap A_j| \pmod{p} \in L\) for all \(i \neq j\), then \(|A| \leq \binom{n}{k}\).

In 1991, Alon, Babai and Suzuki [1] proved the following theorem, which is a generalization of Theorem 1.6 by replacing the condition of uniformity with the condition that the members of \(A\) have \(r\) different sizes.

**Theorem 1.7** (Alon, Babai and Suzuki, 1991 [1]). Let \(K = \{k_1, k_2, \ldots, k_s\}\) and \(L = \{l_1, l_2, \ldots, l_t\}\) be two disjoint subsets of \(\{0, 1, \ldots, p-1\}\), where \(p\) is a prime, and let \(A\) be a family of subsets of \([n]\) such that \(|A_i| \pmod{p} \in K\) for all \(A_i \in A\) and \(|A_i \cap A_j| \pmod{p} \in L\) for \(i \neq j\). If \(r(s - r + 1) \leq p - 1\) and \(n \geq s + \max_{1 \leq i \leq t} k_i\), then \(|A| \leq \binom{n}{k} + \binom{s-1}{k-1} + \cdots + \binom{0}{0}\).

In the proof of Theorem 1.7, Alon, Babai and Suzuki used a very elegant linear algebra method together with their Lemma 3.6 which needs the condition \(r(s - r + 1) \leq p - 1\) and \(n \geq s + \max_{1 \leq i \leq t} k_i\). They conjectured that the condition \(r(s - r + 1) \leq p - 1\) in the statement of their theorem can be dropped off. However, their approach cannot work for this stronger claim. In an effort to prove the Alon-Babai-Suzuki’s conjecture, Snevily [12] obtained the following result.

**Theorem 1.8** (Snevily, 1994 [12]). Let \(p\) be a prime and \(K, L\) be two disjoint subsets of \(\{0, 1, \ldots, p-1\}\). Let \(|L| = s\) and let \(A\) be a family of subsets of \([n]\) such that \(|A_i| \pmod{p} \in K\) for all \(A_i \in A\) and \(|A_i \cap A_j| \pmod{p} \in L\) for \(i \neq j\). Then \(|A| \leq \binom{n}{s} + \binom{s-1}{k-1} + \cdots + \binom{0}{0}\).

Since \(\binom{n-1}{s} + \binom{s-1}{k-1} = \binom{n}{k}\) and \(\binom{s-1}{k-1} \geq \sum_{i=0}^{s-2} \binom{n-1}{i}\) when \(n\) is sufficiently large, Theorem 1.8 not only confirms the conjecture of Alon, Babai and Suzuki in many cases but also strengthens the upper bound of their theorem when \(n\) is sufficiently large.

In 2000, Qian and Ray-Chaudhuri [10] developed a new linear algebra approach and proved the next theorem which shows that the same conclusion in Theorem 1.7 holds if the two conditions \(r(s - r + 1) \leq p - 1\) and \(n \geq s + \max_{1 \leq i \leq r} k_i\) are replaced by a single more relaxed condition \(n \geq 2s - r\).
Theorem 1.9 (Qian and Ray-Chaudhuri, 2000 [10]). Let $p$ be a prime and let $L = \{l_1, l_2, \ldots, l_s\}$ and $K = \{k_1, k_2, \ldots, k_r\}$ be two disjoint subsets of $\{0, 1, \ldots, p-1\}$ such that $n \geq 2s - r$. Suppose that $A$ is a family of subsets of $[n]$ such that $|A_i| \equiv 0 \pmod{p}$ for all $A_i \in A$ and $|A_i \cap A_j| \equiv k \pmod{p}$ for every $i \neq j$. Then $|A| \leq \binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{s-r+1}$.

Recently, Hwang and Kim [8] verified the conjecture of Alon, Babai and Suzuki.

Theorem 1.10 (Hwang and Kim, 2015 [8]). Let $K = \{k_1, k_2, \ldots, k_r\}$ and $L = \{l_1, l_2, \ldots, l_s\}$ be two disjoint subsets of $\{0, 1, \ldots, p-1\}$, where $p$ is a prime, and let $A$ be a family of subsets of $[n]$ such that $|A_i| \equiv 0 \pmod{p}$ for all $A_i \in A$ and $|A_i \cap A_j| \equiv l \pmod{p}$ for every $i \neq j$. If $n \geq s + \max_{1 \leq i \leq r} k_i$, then $|A| \leq \binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{s-r+1}$.

We note here that in some instances Alon, Babai and Suzuki’s condition holds but Qian and Ray-Chaudhuri’s condition does not, while in some other instances the later condition holds but the former condition does not.

In [3], Chen and Liu strengthened the upper bounds of Theorem 1.8 under the condition $\min\{k_i\} > \max\{l_i\}$.

Theorem 1.11 (Chen and Liu, 2009 [3]). Let $p$ be a prime and let $L = \{l_1, l_2, \ldots, l_s\}$ and $K = \{k_1, k_2, \ldots, k_r\}$ be two disjoint subsets of $\{0, 1, \ldots, p-1\}$ such that $\min\{k_i\} > \max\{l_i\}$. Suppose that $A$ is a family of subsets of $[n]$ such that $|A_i| \equiv 0 \pmod{p}$ for all $A_i \in A$ and $|A_i \cap A_j| \equiv l \pmod{p}$ for every $i \neq j$. Then $|A| \leq \binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{s-r+1}$.

In [9], Liu and Yang generalized Theorem 1.11 under a relaxed condition $k_i > s - r$ for every $i$.

Theorem 1.12 (Liu and Yang, 2014 [3]). Let $p$ be a prime and let $L = \{l_1, l_2, \ldots, l_s\}$ and $K = \{k_1, k_2, \ldots, k_r\}$ be two disjoint subsets of $\{0, 1, \ldots, p-1\}$ such that $k_i > s - r$ for every $i$. Suppose that $A$ is a family of subsets of $[n]$ such that $|A_i| \equiv 0 \pmod{p}$ for all $A_i \in A$ and $|A_i \cap A_j| \equiv l \pmod{p}$ for every $i \neq j$. Then $|A| \leq \binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{s-r+1}$.

In the same paper, they also obtained the same bound under the condition of Theorem 1.7.

Theorem 1.13 (Liu and Yang, 2014 [3]). Let $p$ be a prime and let $L = \{l_1, l_2, \ldots, l_s\}$ and $K = \{k_1, k_2, \ldots, k_r\}$ be two disjoint subsets of $\{0, 1, \ldots, p-1\}$ such that $r(s - r + 1) \leq p - 1$ and $n \geq s + \max_{1 \leq i \leq r} k_i$. Suppose that $A$ is a family of subsets of $[n]$ such that $|A_i| \equiv 0 \pmod{p}$ for all $A_i \in A$ and $|A_i \cap A_j| \equiv l \pmod{p}$ for every $i \neq j$. Then $|A| \leq \binom{n-s+1}{s-1} + \binom{n-s+1}{s-2} + \cdots + \binom{n-s+1}{s-r+1}$.

In this paper, we show that Theorem 1.12 still holds under the Alon, Babai and Suzuki’s condition; that is to say, we can drop the condition $r(s - r + 1) \leq p - 1$ in Theorem 1.13.

Theorem 1.14. Let $p$ be a prime and let $L = \{l_1, l_2, \ldots, l_s\}$ and $K = \{k_1, k_2, \ldots, k_r\}$ be two disjoint subsets of $\{0, 1, \ldots, p-1\}$. Suppose that $A$ is a family of subsets of $[n]$ such that $|A_i| \equiv 0 \pmod{p}$ for all $A_i \in A$ and $|A_i \cap A_j| \equiv l \pmod{p}$ for every $i \neq j$. If $n \geq s + \max_{1 \leq i \leq r} k_i$, then $|A| \leq \binom{n-s+1}{s-1} + \binom{n-s+1}{s-2} + \cdots + \binom{n-s+1}{s-r+1}$.

Note that $\binom{n-s+1}{s-1} + \binom{n-s+1}{s-2} + \cdots + \binom{n-s+1}{s-r+1}$ is the upper bound of Alon-Babai-Suzuki’s conjecture (Theorems 1.10) when $n \geq 2s - 2$.

In the proof of Theorem 1.13 we first prove that the bound holds under the condition $n \geq 2s - 2r + 1$, which relaxes the condition $n \geq 2s - r$ in the theorem of Qian and Ray-Chaudhuri.
Let $p$ be a prime and let $L = \{l_1, l_2, \ldots, l_s\}$ and $K = \{k_1, k_2, \ldots, k_r\}$ be two disjoint subsets of $\{0, 1, \ldots, p-1\}$. Suppose that $\mathcal{A}$ is a family of subsets of $[n]$ such that $|A_i| \pmod{p} \in K$ for all $A_i \in \mathcal{A}$ and $|A_i \cap A_j| \pmod{p} \in L$ for every $i \neq j$. If $n \geq 2s - 2r + 1$, then $|\mathcal{A}| \leq \binom{n-1}{s} + \binom{n-1}{2} + \cdots + \binom{n-1}{s-2r+1}$.

Theorems 1.7, 1.9, 1.12 and 1.13 have been extended to $k$-wise $L$-intersecting families in [7, 9]. With a similar idea, our results can also be extended to the $k$-wise case.

2 Proof of Theorem 1.15

In this section we prove Theorem 1.15 which will be helpful in the proof of Theorem 1.14.

Throughout this section, let $X = [n-1] = \{1, 2, \ldots, n-1\}$ be an $(n-1)$-element set, $p$ be a prime, and let $L = \{l_1, l_2, \ldots, l_s\}$ and $K = \{k_1, k_2, \ldots, k_r\}$ be two disjoint subsets of $\{0, 1, \ldots, p-1\}$. Suppose that $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ is a family of subsets of $[n]$ such that $|A_i| \pmod{p} \in K$ for every $1 \leq i \leq m$. (2) $|A_i \cap A_j| \pmod{p} \in L$ for $i \neq j$. Without loss of generality, assume that there exists a positive integer $t$ such that $n \notin A_i$ for $1 \leq i \leq t$ and $n \in A_i$ for $i \geq t+1$. Denote $\mathcal{P}_i(X) = \{S|S \subset X \text{ and } |S| = i\}$.

We associate a variable $x_i$ for each $A_i \in \mathcal{A}$ and set $x = (x_1, x_2, \ldots, x_m)$. For each $I \subset X$, define $L_I = \sum_{i: I \subset A_i} x_i$.

Consider the system of linear equation over the field $\mathbb{F}_p$:

$$\{L_I = 0, \text{ where } I \text{ runs through } \bigcup_{i=0}^s \mathcal{P}_i(X)\}. \tag{1}$$

**Proposition 2.1.** Assume that $L \cap K = \emptyset$. If $\mathcal{A}$ is a $p$ $L$-intersecting family with $|A_i| \pmod{p} \in K$ for every $i$, then the only solution of the above system of linear equations is the trivial solution.

**Proof.** Let $v = (v_1, v_2, \ldots, v_m)$ be a solution to the system \((1)\). We will show that $v$ is the zero solution over the field $\mathbb{F}_p$. Define $g(x) = \prod_{j=1}^s (x - l_j)$, and $h(x) = g(x + 1) = \prod_{j=1}^s (x + 1 - l_j)$.

Since $\binom{x}{0}, \binom{x}{1}, \ldots, \binom{x}{s}$ form a basis for the vector space spanned by all the polynomials in $\mathbb{F}_p[x]$ of degree at most $s$, there exist $a_0, a_1, \ldots, a_s \in \mathbb{F}_p$ and $b_0, b_1, \ldots, b_s \in \mathbb{F}_p$ such that $g(x) = \sum_{i=0}^s a_i \binom{x}{i}$, and $h(x) = \sum_{i=0}^s b_i \binom{x}{i}$.
Let \( A_i \) be an element in \( A \) with \( v_i \neq 0 \). Next we prove the following identities:

If \( n \not\in A_i \), then

\[
\sum_{i=0}^{s} a_i \sum_{I \in \mathcal{P}_i(X), I \subseteq A_i} L_I = \sum_{A_i \in A} g([A_i \cap A_{i_0}]) x_i; \quad (2)
\]

if \( n \in A_i \), then

\[
\sum_{i=0}^{s} b_i \sum_{I \in \mathcal{P}_i(X), I \subseteq A_i} L_I = \sum_{i=1}^{t} h([A_i \cap A_{i_0}]) x_i + \sum_{i \geq t+1} h([A_i \cap A_{i_0}] - 1) x_i. \quad (3)
\]

We prove them by comparing the coefficients of both sides. For any \( A_i \in A \), the coefficient of \( x_i \) in the left hand side of (2) is

\[
\sum_{i=0}^{s} a_i \{ I \in \mathcal{P}_i(X) : I \subseteq A_{i_0}, I \subseteq A_i \} = \sum_{i=0}^{s} a_i \left( |A_i \cap A_{i_0}| \right)_i,
\]

which is equal to \( g([A_i \cap A_{i_0}]) \) by the definition of \( a_i \). This proves the identity (2).

For any \( i \leq t \), the coefficient of \( x_i \) in the left hand side of (3) is

\[
\sum_{i=0}^{s} b_i \{ I \in \mathcal{P}_i(X) : I \subseteq A_{i_0}, I \subseteq A_i \} = \sum_{i=0}^{s} b_i \left( |A_i \cap A_{i_0}| \right)_i,
\]

for any \( i \geq t+1 \), the coefficient of \( x_i \) in the left hand side of (3) is

\[
\sum_{i=0}^{s} b_i \{ I \in \mathcal{P}_i(X) : I \subseteq A_{i_0}, I \subseteq A_i \} = \sum_{i=0}^{s} b_i \left( |A_i \cap A_{i_0}| - 1 \right)_i.
\]

This proves the identity (3).

If \( n \not\in A_{i_0} \), substituting \( x_i \) with \( v_i \) for all \( i \) in the identity (2), we have

\[
\sum_{i=0}^{s} a_i \sum_{I \in \mathcal{P}_i(X), I \subseteq A_{i_0}} L_I(v) = \sum_{A_i \in A} g([A_i \cap A_{i_0}]) v_i.
\]

It is clear that the left hand side is 0 since \( v \) is a solution to (1). For \( A_i \in A \) with \( i \neq i_0 \), \( |A_i \cap A_{i_0}| \pmod{p} \) \( \in L \) and so \( g([A_i \cap A_{i_0}]) = 0 \). Thus the right hand side of the above identity is equal to \( g([A_{i_0}]) v_{i_0} \). So \( g([A_{i_0}]) v_{i_0} = 0 \). Since \( L \cap K = 0 \), we have \( g([A_{i_0}]) \neq 0 \) and so \( v_{i_0} = 0 \). This is a contradiction to the definition of \( v \).

If \( n \in A_{i_0} \), substituting \( x_i \) with \( v_i \) for all \( i \) in the identity (3), we have

\[
\sum_{i=0}^{s} b_i \sum_{I \in \mathcal{P}_i(X), I \subseteq A_{i_0}} L_I(v) = \sum_{i=1}^{t} h([A_i \cap A_{i_0}]) v_i + \sum_{i \geq t+1} h([A_i \cap A_{i_0}] - 1) v_i
\]

\[
= \sum_{i \geq t+1} h([A_i \cap A_{i_0}] - 1) v_i \quad \text{since } v_i = 0 \text{ for all } i \leq t.
\]

Since \( h([A_i \cap A_{i_0}] - 1) = g([A_i \cap A_{i_0}]) \), with a similar argument to the above case, we can deduce the same contradiction. Then the proposition follows. \( \square \)
As a result of this proposition, we have:

\[ |A| \leq \dim(\{ L_I : I \in \bigcup_{i=0}^n \mathbb{P}_i(X) \}), \]

where \( \dim(\{ L_I : I \in \bigcup_{i=0}^n \mathbb{P}_i(X) \}) \) is defined to be the dimension of the space spanned by \( \{ L_I : I \in \bigcup_{i=0}^n \mathbb{P}_i(X) \} \). In the remaining of this section, we make efforts to give an upper bound on this dimension.

**Lemma 2.2.** For any \( i \in \{0, 1, \ldots, s - 2r + 1\} \) and every \( I \in \mathbb{P}_i(X) \), the linear form

\[
\sum_{H \in \mathbb{P}_{i+2r}(X), I \subset H} L_H
\]

is linearly dependent on the set of linear forms \( \{ L_H : i \leq |H| \leq i + 2r - 1, H \subset X \} \) over \( \mathbb{F}_p \).

**Proof.** Define

\[
f(x) = \left( \prod_{j=1}^r (x - (k_j - i)) \right) \times \left( \prod_{j=1}^r (x - (k_j - 1 - i)) \right).
\]

We distinguish two cases.

(a) \( i \ (\text{mod} \ p) \not\in K \) and \( i + 1 \ (\text{mod} \ p) \not\in K \) for all \( i \). In this case \( \forall k_j \in K, k_j - i \neq 0 \) and \( k_j - i - 1 \neq 0 \) in \( \mathbb{F}_p \), and so \( e = (k_1 - i)(k_2 - i) \cdots (k_r - i)(k_1 - i - 1) \cdots (k_r - i - 1) \neq 0 \) in \( \mathbb{F}_p \). It is clear that there exist \( a_1, a_2, \ldots, a_{2r-1} \in \mathbb{F}_p \), \( a_{2r} = (2r)! \in \mathbb{F}_p - \{0\} \) such that

\[
a_1 \left( \frac{x}{1} \right) + a_2 \left( \frac{x}{2} \right) + \cdots + a_{2r} \left( \frac{x}{2r} \right) = f(x) - c,
\]

since the polynomial in the right hand side has constant term equal to 0.

Next we show that

\[
\sum_{j=1}^{2r} a_j \sum_{H \in \mathbb{P}_{i+1}(X), I \subset H} L_H = -cL_I.
\]  \( (4) \)

In fact both sides are linear forms in \( x_A \), for \( A \in A \). The coefficient of \( x_A \) in the left hand side is \( \sum_{j=1}^{2r} a_j |\{ H | I \subset H \subset A, n \not\subset H, |H| = i + j \}| \). So it is equal to

\[
\begin{cases}
0, & \text{if } I \not\subset A; \\
n_1 \left( |A| - i \right) + n_2 \left( |A| - i \right), & \text{if } I \subset A \text{ and } n \not\subset A; \\
n_1 \left( |A| - i - 1 \right) + n_2 \left( |A| - i - 1 \right), & \text{if } I \subset A \text{ and } n \in A.
\end{cases}
\]

By the above polynomial identity,

\[
\sum_{j=1}^{2r} a_j \left( |A| - i \right) = f(|A| - i) - c = -c \text{ since } |A| \ (\text{mod} \ p) \in K;
\]

\[
\sum_{j=1}^{2r} a_j \left( |A| - i - 1 \right) = f(|A| - i - 1) - c = -c \text{ since } |A| \ (\text{mod} \ p) \in K.
\]

The coefficient of \( x_A \) in the right hand side is obviously the same. This proves \( (4) \).
Writing (1) in a different way, we have
\[ \sum_{H \in \mathcal{P}_{i+2r}(X), I \subset H} L_H = -\frac{1}{(2r)!} \left( c L_I + \sum_{j=1}^{2r-1} a_j \sum_{H \in \mathcal{P}_{i+j}(X), I \subset H} L_H \right). \]

This proves the lemma in case (a).

(b) $i \pmod{p} \in K$ or $i + 1 \pmod{p} \in K$ for some $i$. In this case, the constant term of $(x - (k_1 - i))(x - (k_2 - i))\cdots(x - (k_r - i))(x - (k_1 - i - 1))\cdots(x - (k_r - i - 1))$ is 0 in $F_p$.

So there exists $a_1, a_2, \ldots, a_{2r-1} \in F_p$, $a_{2r} = (2r)! \in F_p - \{0\}$ such that
\[ a_1 \left( \frac{x}{1} \right) + a_2 \left( \frac{x}{2} \right) + \cdots + a_{2r} \left( \frac{x}{2r} \right) = f(x) \]

As a consequence we have
\[ \sum_{j=1}^{2r} a_j \sum_{H \in \mathcal{P}_{i+j}(X), I \subset H} L_H = 0 \quad \forall I \in \mathcal{P}_i(X), \]
i.e. we have
\[ \sum_{H \in \mathcal{P}_{i+2r}(X), I \subset H} L_H = -\frac{1}{(2r)!} \left( \sum_{j=1}^{2r-1} a_j \sum_{H \in \mathcal{P}_{i+j}(X), I \subset H} L_H \right). \]

This finishes the proof of this lemma.

\[ \square \]

**Corollary 2.3.** With the same condition as in Lemma 2.2 we have
\[ \langle L_H : H \in \bigcup_{j=1}^{i+2r-1} \mathcal{P}_j(X) \rangle = \langle L_H : H \in \bigcup_{j=i+1}^{i+2r-1} \mathcal{P}_j(X) \rangle + \left\langle \sum_{H \in \mathcal{P}_{i+2r}(X), I \subset H} L_H : I \in \mathcal{P}_i(X) \right\rangle \]

Here $\langle L_H : H \in \bigcup_{j=1}^{i+2r-1} \mathcal{P}_j(X) \rangle$ is the vector space spanned by $\{L_H : H \in \bigcup_{j=i+1}^{i+2r-1} \mathcal{P}_j(X)\}$.

The rest of the proof is similar to the proof of Theorem 1.9 given by Qian and Ray-Chaudhuri [10]. The next lemma is a restatement of [10] Lemma 2, and is used to prove Lemma 2.5.

**Lemma 2.4.** For any positive integers $u, v$ with $u < v < p$ and $u + v \leq n - 1$, we have
\[ \dim \left( \frac{\langle L_J : J \in \mathcal{P}_v(X) \rangle}{\langle \sum_{J \in \mathcal{P}_v(X), I \subset J} L_J : I \in \mathcal{P}_u(X) \rangle} \right) \leq \binom{n-1}{v} - \binom{n-1}{u}, \]

Here $\frac{A}{B}$ is the quotient space of two vector spaces $A$ and $B$ with $B \leq A$.

**Lemma 2.5.** For any $i \in \{0, 1, \ldots, s - 2r + 1\}$,
\[ \binom{n-1}{i} + \binom{n-1}{i+1} + \cdots + \binom{n-1}{i+2r-1} + \dim \left( \frac{\langle L_H : H \in \bigcup_{j=i}^{i+2r-1} \mathcal{P}_j(X) \rangle}{\langle L_H : H \in \bigcup_{j=i}^{i+2r-1} \mathcal{P}_j(X) \rangle} \right) \leq \binom{n-1}{s-2r+1} + \binom{n-1}{s-2r+2} + \cdots + \binom{n-1}{s}. \]
Proof. We induct on \( s - 2r + 1 - i \). It is clearly true when \( s - 2r + 1 - i = 0 \). Suppose the lemma holds for \( s - 2r + 1 - i < l \) for some positive integer \( l \). Now we want to show that it holds for \( s - 2r + 1 - i = l \).

We observe that \( i + i + 2r \leq (s - 2r) + (s - 2r) + 2r \leq n - 1 \) by the condition in the theorem. By Corollary 2.3 and Lemma 2.4, we have

\[
\dim \left( \langle L_H : H \in \cup_{j=1}^{i+2r-1} \mathbb{P}_j(X) \rangle \right) = \dim \left( \langle L_H : H \in \cup_{j=1}^{i+2r-1} \mathbb{P}_j(X) \rangle + \langle L_H : H \in \mathbb{P}_{i+2r}(X) \rangle \right)
\]

\[
\leq \left( \frac{n - 1}{i + 2r} \right) - \left( \frac{n - 1}{i} \right)
\]

Now we are ready to prove the lemma.

\[
\left( \frac{n - 1}{i} \right) + \left( \frac{n - 1}{i + 1} \right) + \cdots + \left( \frac{n - 1}{i + 2r - 1} \right) + \dim \left( \langle L_H : H \in \cup_{j=1}^{i+2r-1} \mathbb{P}_j(X) \rangle \right) = \dim \left( \langle L_H : H \in \cup_{j=1}^{i+2r-1} \mathbb{P}_j(X) \rangle \right)
\]

By Corollary 2.3 and Lemma 2.4, we have

\[
\dim \left( \langle L_H : H \in \cup_{j=1}^{i+2r-1} \mathbb{P}_j(X) \rangle + \langle L_H : H \in \mathbb{P}_{i+2r}(X) \rangle \right)
\]

\[
\leq \left( \frac{n - 1}{i + 2r} \right) - \left( \frac{n - 1}{i} \right)
\]

where the last step follows from the induction hypothesis since \( s - 2r + 1 - (i + 1) < l \). \( \square \)
We are now turning to the proof of Theorem 1.15.

Proof.

\[ |A| \leq \dim((L_H : H \in \bigcup_{i=0}^r \mathbb{P}_i(X))) \]
\[ \leq \dim((L_H : H \in \bigcup_{i=0}^{r-1} \mathbb{P}_i(X))) + \dim \left( \frac{\{L_H : H \in \bigcup_{i=0}^r \mathbb{P}_i(X)\}}{\{L_H : H \in \bigcup_{i=0}^{r-1} \mathbb{P}_i(X)\}} \right) \]
\[ \leq \binom{n-1}{0} + \binom{n-1}{1} + \cdots + \binom{n-1}{2r-1} + \dim \left( \frac{\{L_H : H \in \bigcup_{i=0}^r \mathbb{P}_i(X)\}}{\{L_H : H \in \bigcup_{i=0}^{r-1} \mathbb{P}_i(X)\}} \right) \]
\[ \leq \left( \frac{n-1}{s-2r+1} \right) + \left( \frac{n-1}{s-2r+2} \right) + \cdots + \left( \frac{n-1}{s} \right) \]
by taking \( i = 0 \) in Lemma 2.5

which completes the proof of the theorem. \( \square \)

3 Proof of Theorem 1.14

Throughout this section, we let \( p \) be a prime and we will use \( x = (x_1, x_2, \ldots, x_n) \) to denote a vector of \( n \) variables with each variable \( x_i \) taking values 0 or 1. A polynomial \( f(x) \) in \( n \) variables \( x_i \), for \( 1 \leq i \leq n \), is called multilinear if the power of each variable \( x_i \) in each term is at most one. Clearly, if each variable \( x_i \) only takes the values 0 or 1, then any polynomial in variable \( x \) can be regarded as multilinear. For a subset \( A \) of \( \{n\} \), we define the incidence vector \( v_A \) of \( A \) to be the vector \( v = (v_1, v_2, \ldots, v_n) \) with \( v_i = 1 \) if \( i \in A \) and \( v_i = 0 \) otherwise.

Let \( L = \{l_1, l_2, \ldots, l_s\} \) and \( K = \{k_1, k_2, \ldots, k_t\} \) be two disjoint subsets of \( \{0, 1, \ldots, p-1\} \), where the elements of \( K \) are arranged in increasing order. Suppose that \( A = \{A_1, \ldots, A_m\} \) is the family of subsets of \( \{n\} \) satisfying the conditions in Theorem 1.14. Without loss of generality, we may assume that \( n \in A_j \) for \( j \geq t+1 \) and \( n \notin A_j \) for \( 1 \leq j \leq t \).

For each \( A_j \in A \), define
\[ f_{A_j}(x) = \prod_{i=1}^s (v_{A_j} - x_i), \]
where \( x = (x_1, x_2, \ldots, x_n) \) is a vector of \( n \) variables with each variable \( x_i \) taking values 0 or 1. Then each \( f_{A_j}(x) \) is a multilinear polynomial of degree at most \( s \).

Let \( Q \) be the family of subsets of \( \{n-1\} \) with size at most \( s-1 \). Then \( |Q| = \sum_{i=0}^{s-1} \binom{n-1}{i} \).

For each \( L \in Q \), define
\[ q_L(x) = (1 - x_n) \prod_{i \in L} x_i. \]
Then each \( q_L(x) \) is a multilinear polynomial of degree at most \( s \).

Denote \( K - 1 = \{k_j - 1 | k_j \in K\} \). Then \( |K \cup (K - 1)| \leq 2r \). Set
\[ g(x) = \prod_{h \in K \cup (K - 1)} \left( \sum_{i=1}^{n-1} x_i - h \right). \]
Let \( W \) be the family of subsets of \( \{n-1\} \) with size at most \( s - 2r \). Then \( |W| = \sum_{i=0}^{s-2r} \binom{n-1}{i} \).

For each \( I \in W \), define
\[ g_I(x) = g(x) \prod_{i \in I} x_i. \]
Then each \( g_I(x) \) is a multilinear polynomial of degree at most \( s \).
We want to show that the polynomials in
\[ \{ f_{A_i}(x) \mid 1 \leq i \leq m \} \cup \{ q_L(x) \mid L \in Q \} \cup \{ g_I(x) \mid I \in W \} \]
are linearly independent over the field \( F_p \). Suppose that we have a linear combination of these polynomials that equals 0:
\[ \sum_{i=1}^{m} a_i f_{A_i}(x) + \sum_{L \in Q} b_L q_L(x) + \sum_{I \in W} u_I g_I(x) = 0, \tag{5} \]
with all coefficients \( a_i, b_L \) and \( u_I \) being in \( F_p \).

**Claim 1.** \( a_i = 0 \) for each \( i \) with \( n \notin A_i \).

Suppose, to the contrary, that \( i_0 \) is a subscript such that \( n \notin A_{i_0} \) and \( a_{i_0} \neq 0 \). Since \( n \notin A_{i_0} \), \( q_L(v_{A_{i_0}}) = 0 \) for every \( L \in Q \). Recall that \( f_{A_j}(v_{i_0}) = 0 \) for \( j \neq i_0 \) and \( g(v_{i_0}) = 0 \). By evaluating \( f_{A_j}(v_{i_0}) = 0 \) for \( j \neq i_0 \) and \( g(v_{i_0}) = 0 \). Since \( f_{A_{i_0}}(v_{A_{i_0}}) \neq 0 \), we have \( a_{i_0} = 0 \), a contradiction. Thus, Claim 1 holds.

**Claim 2.** \( a_i = 0 \) for each \( i \) with \( n \notin A_i \). Applying Claim 1, we get
\[ \sum_{i=1}^{m} a_i f_{A_i}(x) + \sum_{L \in Q} b_L q_L(x) + \sum_{I \in W} u_I g_I(x) = 0. \tag{6} \]

Suppose, to the contrary, that \( i_0 \) is a subscript such that \( n \notin A_{i_0} \) and \( a_{i_0} \neq 0 \). Let \( v'_{i_0} = v_{i_0} + (0, 0, \ldots, 0, 1) \). Then \( q_L(v'_{i_0}) = 0 \) for every \( L \in Q \). Note that \( f_{A_j}(v'_{i_0}) = f_{A_j}(v_{i_0}) \) for each \( j \) with \( n \notin A_j \) and \( g(v'_{i_0}) = 0 \). By evaluating \( f_{A_j}(v'_{i_0}) = f_{A_j}(v_{i_0}) \) for each \( j \) with \( n \notin A_j \) and \( g(v'_{i_0}) = 0 \). Since \( f_{A_{i_0}}(v_{A_{i_0}}) \neq 0 \) (mod \( p \)) which implies \( a_{i_0} = 0 \), a contradiction. Thus, the claim is verified.

**Claim 3.** \( b_L = 0 \) for each \( L \in Q \).

By Claims 1 and 2, we obtain
\[ \sum_{L \in Q} b_L q_L(x) + \sum_{I \in W} u_I g_I(x) = 0. \tag{7} \]

Set \( x_n = 0 \) in \( \tag{7}, \) then
\[ \sum_{L \in Q} b_L \prod_{i \in L} x_i + \sum_{I \in W} u_I g_I(x) = 0. \]

Subtracting the above equality from \( \tag{7}, \) we get
\[ \sum_{L \in Q} b_L \left( x_n \prod_{i \in L} x_i \right) = 0. \]

Setting \( x_n = 1 \), we obtain
\[ \sum_{L \in Q} b_L \prod_{i \in L} x_i = 0. \]

It is not difficult to see that the polynomials \( \prod_{i \in L} x_i, L \in Q \), are linearly independent. Therefore, we conclude that \( b_L = 0 \) for each \( L \in Q \).

By Claims 1-3, we now have
\[ \sum_{I \in W} u_I g_I(x) = 0. \]

Thus it is sufficient to prove \( g_I \)'s are linearly independent.
Let $N$ be a positive integer and $H = \{h_1, h_2, \ldots, h_u\}$ be a subset of $[N]$ with all the elements being arranged in increasing order. We say $H$ has a gap of size $g$ if either $h_1 \geq g - 1, N - h_u \geq g - 1$, or $h_{i + 1} - h_i \geq g$ for some $i$ ($1 \leq i \leq u - 1$). The following result obtained by Alon, Babai, and Suzuki is critical to our proof.

**Lemma 3.1.** Let $H$ be a subset of $\{0, 1, \ldots, p - 1\}$. Let $p(x)$ denote the polynomial function defined by $p(x) = \prod_{h \in H} (x + x_2 + \cdots + x_N - h)$. If the set $(H + pZ) \cap [N]$ has a gap $g \geq 1$, where $g$ is a positive integer, then the set of polynomials $\{p_I(x) : |I| \leq g - 1, I \in H\}$ is linearly independent over $\mathbb{F}_p$, where $p_I(x) = p(x) \prod_{i \in I} x_i$.

To apply Lemma 3.1, we define the set $H$ as follows: $H = (K \cup (K - 1) + pZ) \cap [n - 1]$. We can divide $n - 1$ into the following four cases:

1. $s + k_r - 1 \leq n - 1 < p + k_1 - 1$;
2. $s + k_r - 1 < p + k_1 - 1 \leq n - 1$;
3. $(s - 2r + 1) + k_r < p + k_1 - 1 \leq s + k_r - 1 \leq n - 1$;
4. $p + k_1 - 1 \leq (s - 2r + 1) + k_r \leq s + k_r - 1 \leq n - 1$.

**Case 1:** $s + k_r - 1 \leq n - 1 < p + k_1 - 1$.

Since $n - 1 < p + k_1 - 1$, the set $H$ consists of only $\{k_1 - 1, k_1, \ldots, k_r\}$. From $s + k_r - 1 \leq n - 1$, we obtain $n - 1 - k_r \geq s - 1 \geq s - 2r + 1$. By the definition of the gap, $H$ has a gap $\geq s - 2r + 2$.

**Case 2:** $s + k_r - 1 < p + k_1 - 1 \leq n - 1$.

Since $n - 1 \geq p + k_1 - 1$, the set $H$ contains at least the following elements $\{k_1 - 1, k_1, \ldots, k_r, p + k_1 - 1\}$. From $s + k_r - 1 < p + k_1 - 1$, we derive $(p + k_1 - 1) - k_r \geq s - 2r + 2$. Thus, $H$ has a gap $\geq s - 2r + 2$.

**Case 3:** $(s - 2r + 1) + k_r < p + k_1 - 1 \leq s + k_r - 1 \leq n - 1$.

Since $n - 1 \geq p + k_1 - 1$, $H$ contains at least the following elements $\{k_1 - 1, k_1, \ldots, k_r, p + k_1 - 1\}$. Since $(s - 2r + 1) + k_r < p + k_1 - 1$, we have $(p + k_1 - 1) - k_r \geq s - 2r + 1$. Then $H$ has a gap $\geq s - 2r + 2$.

By applying Lemma 3.1 we conclude that the set of polynomials $\{g_I(x) : I \in W\}$ is linearly independent over $\mathbb{F}_p$, and so $u_I = 0$ for each $I \in W$.

In summary, for the Cases 1–3, we have shown that the polynomials in

$$\{f_{A_i}(x) : 1 \leq i \leq m\} \cup \{q_L(x) : L \in Q\} \cup \{g_I(x) : I \in W\}$$

are linearly independent over the field $\mathbb{F}_p$. Since the set of all monomials in variables $x_1, x_2, \ldots, x_n$ of degree at most $s$ forms a basis for the vector space of multilinear polynomials of degree at most $s$, it follows that

$$|A| + \sum_{i=0}^{s-1} \binom{n-1}{i} + \sum_{i=0}^{2r-1} \binom{n-1}{i} \leq \sum_{i=0}^{s} \binom{n}{i},$$

which implies that

$$|A| \leq \binom{n-1}{s} + \binom{n-1}{s-1} + \cdots + \binom{n-1}{s-2r+1}.$$

This completes the proof of the theorem for the Cases 1–3.

Since Theorem 1.15 has shown that the statement of Theorem 1.14 remains true under the condition $n \geq 2s - 2r + 1$, we just consider $n \leq 2s - 2r$ for the Case 4. The following argument is similar to the technique Hwang and Kim used for the proof of Alon-Babai-Suzuki's conjecture.
Since \( p + k_1 - 1 \leq (s - 2r + 1) + k_r \leq s + k_r - 1 \leq n - 1 \leq 2s - 2r - 1 \), we obtain \( k_r \leq s - 2r \).

Thus, we have \( r + s \leq p \leq s - 2r + 2 + k_r - k_1 \leq 2s - 4r + 1 \). This implies \( s \geq 5r - 1 \).

Since \( n \leq 2s - 2r < 2p \), we have \(|A| \in (K + p\mathbb{Z}) \cap [n] = \{k_1, k_2, \ldots, k_r, p + k_1, \ldots, p + k_c\}\) for some \( 1 \leq c \leq r \). This gives

\[
|A| \leq \binom{n}{k_1} + \binom{n}{k_2} + \cdots + \binom{n}{k_r} + \binom{n}{p + k_1} + \cdots + \binom{n}{p + k_c}.
\]

We will show that the right hand side of the above inequality is less than or equal to \( \binom{n-1}{s-1} + \binom{n-1}{s-2} + \cdots + \binom{n-1}{s-2r+1} \). Since \( s + r + k_1 - 1 \leq p + k_1 - 1 \leq (s - 2r + 1) + k_r \), we have \( k_r \geq 3r - 2 + k_1 \). Let \( n = 2s - 2r - \delta \) for integer \( \delta \), where \( 0 \leq \delta \leq s - 5r + 1 \), since \( 2s - 2r \geq n \geq s + k_r \geq s + 3r - 2 + k_1 \). Since the sequence \( \{\binom{n}{k}\} \) is unimodal and symmetric around \( n/2 \), we have \( |s - n/2| = r + \delta/2 > r - \delta/2 - 2 = |n/2 - (s - 2r + 2)| \).

Therefore we have

\[
\min\left[\binom{n}{s}, \binom{n}{s-2}, \ldots, \binom{n}{s-2r+2}\right] = \binom{n}{s}. \tag{8}
\]

Since \( n = 2s - 2r - \delta \geq p + k_c \geq r + s + k_c \), we have \( k_c \leq s - 3r - \delta \). For \( 1 \leq i \leq c \), \( k_i \) can be written as \( k_i = s - 3r - \delta - a_i \), where \( 0 \leq a_i \leq s - 3r - \delta \). Thus, we have \( p + k_i \geq r + s + k_i = 2s - 2r - \delta - a_i \), where \( 1 \leq i \leq c \). Since \( 2s - 2r - \delta - a_i \geq s + r > n/2 \), we have

\[
\sum_{i=1}^{c} \left( \binom{n}{k_i} + \binom{n}{p + k_i} \right) \leq \sum_{i=1}^{c} \left( \binom{n}{s - 3r - \delta - a_i} + \binom{n}{2s - 2r - \delta - a_i} \right).
\]

For \( c + 1 \leq i \leq r \), we derive \( k_i \leq k_c < s - 2r - \delta < n/2 \). Noting that \( |s - n/2| = r + \delta/2 = |n/2 - (s - 2r - \delta)| \), we have \( \binom{n}{k} \leq \binom{n}{s} \) for all \( c + 1 \leq i \leq r \). Then

\[
|A| \leq \sum_{i=1}^{c} \left( \binom{n}{k_i} + \binom{n}{p + k_i} \right) + \sum_{i=c+1}^{r} \binom{n}{k_i},
\]

with the help of the next lemma, we can complete our proof.

**Lemma 3.2.** [\( \star \)] For all \( 0 \leq c < k \leq n/2 \), we have

\[
\binom{n}{k-1-c} + \binom{n}{c} \leq \binom{n}{k}.
\]

Let \( k = n - s = s - 2r - \delta < n/2 \), apply Lemma 3.2. For every \( 0 \leq a \leq s - 3r - \delta < k \), we have

\[
\binom{n}{s - 3r - \delta - a} + \binom{n}{2s - 2r - \delta - a} = \binom{n}{s - r - a} + \binom{n}{n - a} = \binom{n}{k - r - a} + \binom{n}{a} \leq \binom{n}{k - 1 - a} + \binom{n}{a} \leq \binom{n}{k} = \binom{n}{s}.
\]
We now finish the proof of Theorem 1.14 for the Case 4.

\[
|A| \leq \sum_{i=1}^{c} \left( \binom{n}{s - 3r - \delta - a_i} + \binom{n}{2s - 2r - \delta - a_i} \right) + (r - c) \binom{n}{s} \leq r \binom{n}{s}.
\]

By (8), we have

\[
|A| \leq \binom{n}{s} + \binom{n}{s - 2} + \cdots + \binom{n}{s - 2r + 2} = \binom{n - 1}{s} + \binom{n - 1}{s - 1} + \cdots + \binom{n - 1}{s - 2r + 1}.
\]

Acknowledgements

The research of G. Ge was supported by the National Natural Science Foundation of China under Grant Nos. 61171198, 11431003 and 61571310, and the Importation and Development of High-Caliber Talents Project of Beijing Municipal Institutions.

References

[1] N. Alon, L. Babai, and H. Suzuki. Multilinear polynomials and Frankl–Ray-Chaudhuri–Wilson type intersection theorems. J. Combin. Theory Ser. A, 58(2):165–180, 1991.

[2] R. C. Bose. A note on Fisher’s inequality for balanced incomplete block designs. Ann. Math. Statistics, 20:619–620, 1949.

[3] W. Y. C. Chen and J. Liu. Set systems with \(L\)-intersections modulo a prime number. J. Combin. Theory Ser. A, 116(1):120–131, 2009.

[4] N. G. de Bruijn and P. Erdős. On a combinatorial problem. Nederl. Akad. Wetensch., Proc., 51:1277–1279 = Indagationes Math. 10, 421–423 (1948), 1948.

[5] P. Erdős, C. Ko, and R. Rado. Intersection theorems for systems of finite sets. Quart. J. Math. Oxford Ser. (2), 12:313–320, 1961.

[6] P. Frankl and R. M. Wilson. Intersection theorems with geometric consequences. Combinatorica, 1(4):357–368, 1981.

[7] V. Grolmusz and B. Sudakov. On \(k\)-wise set-intersections and \(k\)-wise Hamming-distances. J. Combin. Theory Ser. A, 99(1):180–190, 2002.

[8] K.-W. Hwang and Y. Kim. A proof of Alon-Babai-Suzuki’s conjecture and multilinear polynomials. European J. Combin., 43:289–294, 2015.

[9] J. Liu and W. Yang. Set systems with restricted \(k\)-wise \(L\)-intersections modulo a prime number. European J. Combin., 36:707–719, 2014.

[10] J. Qian and D. K. Ray-Chaudhuri. On mod-\(p\) Alon-Babai-Suzuki inequality. J. Algebraic Combin., 12(1):85–93, 2000.

[11] D. K. Ray-Chaudhuri and R. M. Wilson. On \(t\)-designs. Osaka J. Math., 12(3):737–744, 1975.

[12] H. S. Snevily. On generalizations of the de Bruijn-Erdős theorem. J. Combin. Theory Ser. A, 68(1):232–238, 1994.