Number of sets with small sumset and the clique number of random Cayley graphs

Gyan Prakash

Abstract

Let $G$ be a finite abelian group of order $n$. For any subset $B$ of $G$ with $B = -B$, the Cayley graph $G_B$ is a graph on vertex set $G$ in which $i j$ is an edge if and only if $i - j \in B$. It was shown by Ben Green [6] that when $G$ is a vector space over a finite field $\mathbb{Z}/p\mathbb{Z}$, then there is a Cayley graph containing neither a complete subgraph nor an independent set of size more than $c \log n \log \log n$, where $c > 0$ is an absolute constant. In this article we observe that a modification of his arguments shows that for an arbitrary finite abelian group of order $n$, there is a Cayley graph containing neither a complete subgraph nor an independent set of size more than $c (\omega^2(n) \log \omega(n) + \log n \log \log n)$, where $c > 0$ is an absolute constant and $\omega(n)$ denotes the number of distinct prime divisors of $n$.

A graph $G = (V, E)$ consists of a finite nonempty set $V$ (vertex set) together with a prescribed set $E$ (edge set) of unordered pair of distinct elements of $V$. Each pair $x = \{u, v\} \in E$ is an edge of $G$ and $x$ is said to join $u$ and $v$ by an edge. The graph $G$ is complete if any two elements in $V$ are joined by an edge. A maximal complete subgraph of a graph is a clique and the clique number is the maximal order of a clique. An independent set of a graph $G = (V, E)$ is a subset $V'$ of $V$ such that no two points in $V'$ are connected by an edge. Given a graph $G = (V, E)$ the complementary graph $G^c = (V', E')$ is a graph with vertex set $V' = V$ and two elements of $V$ are joined by an edge in $G^c$ if and only if they are not joined by an edge in $G$. A set is an independent set in $G$ if and only if it spans a complete subgraph in $G^c$.

Ramsey proved that given any positive integer $k$, there is a Ramsey number $R(k)$ such that any graph $G$ on $n$ vertices, with $n \geq R(k)$, contains either a clique or an independent set which has more than $k$ vertices. Erdős [8] showed that the Ramsey number $R(k)$ has at least an exponential growth in $k$. Using a probabilistic argument, Erdős proved that there exists a graph on $n$ vertices which neither contains a clique nor an independent set of size more than $c \log n$ vertices with $c$ being a positive absolute constant. An explicit construction of such a graph is not known. Chung [5] gave a construction of graphs on $n$ vertices which contains neither a complete subgraph nor an independent set on more than $e^{c \log n}^{3/4} / (\log \log n)^{1/4}$ vertices.
Given a finite abelian group \( G \) of order \( n \) and a set \( B \subset G \), with \( B = -B \) and \( 0 \not\in B \), the Cayley graph \( G_B \) is a graph on vertex set \( G \) in which \( ij \) is an edge if and only if \( i - j \in B \). It is expected that for most of primes \( q \) with \( q \equiv 1 \mod (4) \) the Paley graphs \( P_q \), which is a Cayley graph \( G_B \) with \( G = \mathbb{Z}/q\mathbb{Z} \) and \( B \) being a set of quadratic residues, is an example of a graph which contains neither a clique nor an independent set on more than \( c \log n \) vertices. However this is far from being proven and is expected to be a very difficult problem. It is easy to see that a lower bound for clique number of \( P_q \) is \( \frac{n(q)}{q} \), where \( n(q) \) denotes the least positive integer which is a quadratic nonresidue modulo \( q \). The best unconditional upper bound known for \( n(q) \) is \( q^{1/4\sqrt{e}+\epsilon} \) and under the assumption of generalised Riemann hypothesis one knows that \( n(q) \) is at most \( c \log^2 q \). The best known upper bound for clique number of \( P_q \) to our knowledge is \( \sqrt{q} \) [4, page 363, Theorem 13.14]. One may ask whether among Cayley graphs, there are graphs (not necessarily Paley graphs) which contains neither a complete subgraph nor an independent set of very large order. The following conjecture is due to Noga Alon.

**Conjecture 1.** [1] Conjecture 4.1 There exists an absolute constant \( b \) such that the following holds. For every group \( G \) on \( n \) elements there exists a set \( B \subset G \) such that the Cayley graph \( G_B \) neither contains a complete subgraph nor an independent set on more than \( b \log n \) vertices.

For the relation between this conjecture and certain other questions in information theory, one may see the article of Noga Alon [1]. A weaker version of this conjecture, obtained by replacing the term \( \log n \) by \( \log^2 n \), was proved by N. Alon and A. Orilitsky in [2].

Ben Green [6] proved the above conjecture in the case when \( G \) is cyclic. In the case when \( G = (\mathbb{Z}/p\mathbb{Z})^r \) with \( p \) being a prime, he proved a weaker version of the above conjecture with the term \( \log n \) replaced by \( \log n \log \log n \). It was shown by Green that if we select a subset \( B \) of \( G \) randomly, then almost surely the Cayley graph \( G_B \) contains neither a complete subgraph nor an independent set of large size. On the other hand, Green also proved that when \( G = (\mathbb{Z}/2\mathbb{Z})^r \), then for a random subset \( B \), the Cayley graph \( G_B \) almost surely contains a complete subgraph of size at least \( c \log n \log \log n \) and thus showing that the random methods alone can not prove the above conjecture for a general finite abelian groups. Moreover Ben Green remarked in [6] that his methods seems to work only for certain special groups.

In this article we observe that a modification of the arguments from [6] prove the following weaker version of the above conjecture for any finite abelian group.

**Theorem 2.** Let \( G \) be a finite abelian group of order \( n \). Then there exist a subset \( B \) of \( G \) with \( B = -B \) and \( 0 \notin B \), such that the Cayley graph \( G_B \) neither contains a complete subgraph nor an independent set on more than...
Theorem 3. There exists an absolute constant after a minimal modification gives the same result for Cayley graphs and not for Cayley graphs. However as he remarked, his arguments denote the clique number of the Cayley graph $G$ by Ben Green [6, Theorem 9], whereas we prove it for an arbitrary finite abelian group $G$.

In case $G = (\mathbb{Z}/p\mathbb{Z})^r$, then $\omega(n) = 1$ and we obtain the result of Ben Green mentioned above. Since sometimes $\omega(n)$ could be as large as $\log n \log \log n$, which happens when $n$ has several small prime divisors, it is not possible to recover the result of Alon and Orilitsky from Theorem 3. When $\omega(n) = 1$, we recover the result of Theorem 3. When $\omega(n)$ is of the order $\log n \log \log n$, then taking $\alpha = 1$, we obtain the bound $c_1(\log n \log \log n)^2$.

The complementary graph of a Cayley graph $G_B$ is the Cayley graph $G_B^c$ with $B^c = G \setminus (B \cup \{0\})$. Thus to prove Theorem 2 we need to show the existence of set $B \subset G$ such that the clique number of $G_B$ as well as that of $G_B^c$ is small. We divide $G \setminus \{0\}$ into disjoint pairs of the form $(g, -g)$ with $g \in G \setminus \{0\}$. Then we choose a subset $B$ of $G$ randomly by choosing each such pair in $B$ independently with probability $1/2$. We write $cl(B)$ to denote the clique number of the Cayley graph $G_B$.

In case $G = (\mathbb{Z}/p\mathbb{Z})^r$ with $p$ being a prime, the following result was proved by Ben Green [6, Theorem 9], whereas we prove it for an arbitrary finite abelian group $G$. Green had stated and proved his results for Cayley sum graphs and not for Cayley graphs. However as he remarked, his arguments after a minimal modification gives the same result for Cayley graphs.

Theorem 3. There exists an absolute constant $c_1 > 0$ such that the following holds. For any finite abelian group $G$ of order $n$ we have that

$$\lim_{n \to \infty} \mathbb{P}\left( cl(B) \geq c_1(\omega^3(n) \log \omega(n) + \log n \log \log n) \right) = 0.$$ 

Remark 4. Using the arguments of this paper and the result [6, Proposition 19] proved by Green, one can show that the clique number of random Cayley graph is at most $c_1\omega^3(\log n \log \omega(n) + (\log n \log \log n)^{1+\alpha})$ for any $\alpha \in [0, 1]$. When $\omega(n) \leq \log n^{1/3}$, the choice of $\alpha = 0$ is optimal. Taking $\alpha = 0$, we recover the result of Theorem 3. When $\omega(n)$ is of the order $\log n \log \log n$, then taking $\alpha = 1$, we obtain the bound $c_1(\log n \log \log n)^2$.

We observe that Theorem 2 follows immediately from Theorem 3 using the following inequality:

$$\mathbb{P}(cl(B) \geq k_1 \text{ or } cl(B^c) \geq k_1) \leq \mathbb{P}(cl(B) \geq k_1) + \mathbb{P}(cl(B^c) \geq k_1) = 2\mathbb{P}(cl(B) \geq k_1),$$

where the last equality follows using the fact that for any pair $\{g, -g\}$ with $g \in G \setminus \{0\}$, the probability that the pair belongs to $B$ is equal to the probability that it belongs to $B^c$.

For any positive integers $k_1$ and $k_2$ we set

$$S^-(k_1, k_2, G) = \{ A \subset G : \text{card}(A) = k_1, \text{card}(A - A) = k_2 \},$$

(1)
Theorem 5. [6, Proposition 26] For any prime \( p \) the arguments give the same result when \( A \) be written as a difference of two elements from \( G \), of the form (1, complete subgraph is at most \( S \) the arguments gives the same upper bound for \( \text{card}(S) \) graph and the cardinality of \( P \) if \( k \) if \( A \) is a positive absolute constant. Presently, we recall the arguments from [6] which prove (2). The probability that the clique number \( cl(B) \) of a random Cayley graph \( G_B \) is greater than or equal to \( k_1 \) is same as the probability that there exist a set \( A \subset G \) with \( \text{card}(A) = k_1 \) which spans a complete subgraph in \( G_B \). The subgraph of \( G_B \) spanned by the vertices of \( A \) is complete if and only if \( (A - A) \setminus \{0\} \) is a subset of \( B \). If \( \text{card}(A - A) = k_2 \), it contains at least \( \frac{k_1}{2} + 1 \) disjoint pairs of the form \( (g, -g) \) with \( g \in G \setminus \{0\} \). Thus the probability that \( A \) spans a complete subgraph is at most \( \frac{1}{2^{k_2 + 1}} \). Therefore we have

\[
\mathbb{P}(cl(B) \geq k_1) \leq \sum_{k_2 \geq k_1} \sum_{A \in S^{(k_1,k_2)}(G)} \mathbb{P}((A - A) \setminus \{0\} \subset B) \leq \sum_{k_2 \geq k_1} \frac{\text{Card}(S^{(k_1,k_2)}(G))}{2^{(k_2-1)/2}}.
\]

For any positive integers \( k_1 \) and \( k_2 \) we also set

\[
S(k_1, k_2, G) = \{ A \subset G : \text{card}(A) = k_1, \text{card}(A \hat{\cup} A) \leq k_2 \},
\]

where \( A \hat{\cup} A \) denotes those elements of \( G \) which can be written as a sum of two distinct elements of \( A \).

The following result was stated in [6] when \( G = (\mathbb{Z}/p\mathbb{Z})^r \) with \( p = 2 \), but the arguments give the same result when \( p \) is an arbitrary prime. Moreover the arguments gives the same upper bound for \( \text{card}(S^{(k_1,k_2)}(\mathbb{Z}/p\mathbb{Z})^r) \).

**Theorem 5.** [6, Proposition 26] For any prime \( p \), we have,

\[
\text{Card}(S(k_1, k_2, (\mathbb{Z}/p\mathbb{Z})^r)) \leq n \frac{4k_2 \log k_1}{k_1} \left( \frac{ek_2}{k_1} \right)^{k_1} \exp(k_1^{3/32})
\]

if \( k_2 \leq k_1^{31/30} \) and

\[
\text{Card}(S(k_1, k_2, (\mathbb{Z}/p\mathbb{Z})^r)) \leq n \frac{4k_2 \log k_1}{k_1} k_1^{4k_1}
\]

for all \( k_2 \). (Here \( n = p^r \) is the order of \( (\mathbb{Z}/p\mathbb{Z})^r \).)

We prove the following result.

**Theorem 6.** Let \( G \) be a finite abelian group of order \( n \). Then the cardinality of \( S^{(k_1,k_2)}(G) \) as well as the cardinality of \( S(k_1, k_2, G) \) is at most

\[
n \frac{4k_2 \log k_1}{k_1} \min(k_1^{c\omega(n)(k_1k_2)^{1/3} \log k_1} \left( \frac{k_2}{k_1 - 1} \right), k_1^{4\omega(n)k_1}),
\]

where \( c \) is a positive absolute constant.
To prove Theorem 5, Green proved the following:

(i) an upper bound for the number of Freiman 2-isomorphism class of sets in \( S(k_1, k_2, G) \),

(ii) an upper bound for the cardinality of the set \( \text{Hom}_2(A, G) \), where \( \text{Hom}_2(A, G) \) consists of all Freiman homomorphism from \( A \) into \( G \),

when \( G = (\mathbb{Z}/p\mathbb{Z})^r \). We prove Theorem 6 by proving the same for general \( G \).

For obtaining an upper bound for \( \text{card}(\text{Hom}_2(A, G)) \), we observe that \( A \) is Freiman 2-isomorphic to a subset \( A_{r,2} \) of a possibly different group \( G' \) such that \( A_{r,2} \) have the following “universal” property. Any Freiman 2-homomorphism from \( A_{r,2} \) into \( G \) extends as a group homomorphism from the group \( \langle A_{r,2} \rangle \) into \( G \), where \( \langle A_{r,2} \rangle \) is the subgroup of \( G' \) generated by \( A_{r,2} \).

Hence the group \( \text{Hom}_2(A_{r,2}, G) \) is isomorphic to \( \text{Hom}(\langle A_{r,2} \rangle, G) \) (Lemma 8), where \( \text{Hom}(\langle A_{r,2} \rangle, G) \) is the group consisting of all group homomorphism from \( \langle A_{r,2} \rangle \) into \( G \). This shows that \( \text{card}(\text{Hom}_2(A, G)) \leq n^{r(\langle A_{r,2} \rangle)} \), where \( r(\langle A_{r,2} \rangle) \) is the rank of the group \( \langle A_{r,2} \rangle \). An upper bound for the rank of \( \langle A_{r,2} \rangle \) follows from a result proved by Green. The arguments used by Green in obtaining an upper bound for the number of Freiman 2-isomorphism classes of sets works for general \( G \) without much difficulty. We need to use Lemma 11 which follows from a standard inductive argument.

Given a positive integer \( s \), for any finite subset \( A \) of an \( F \)-module with \( F \) being one of the following two rings \( \mathbb{Z}/m\mathbb{Z} \) and \( \mathbb{Q} \), in Section 3 we define the Freiman \( s \)-rank \( r_s(A) \) to be the rank of the module \( \text{Hom}_s(A, F) \). We prove Corollary 24 which generalises the result [6, Corollary 14] proved in the case of \( F \) being a field. Although we do not require Corollary 24 to prove other results of this article, the result may be of an independent interest. The result shows that in case \( F = \mathbb{Q} \), the Freiman 2-rank of \( A \) as defined above is same as the rank of \( A \) as defined by Freiman. Using this fact Green observed that the factor \( n^{\frac{4k_1 \log k_2}{k_1^2}} \) in \([1]\) could be improved to \( n^{\frac{4k_2}{k_1}} \) for a cyclic group, which allowed him to prove Conjecture 1 for cyclic groups.

1 Number of sets with small sumset

Let \( m \) be a fixed positive integer. In the sequel, we fix \( F \) to be either \( \mathbb{Z}/m\mathbb{Z} \) or \( \mathbb{Q} \). Let \( M \) be a finitely generated \( F \)-module. If \( F = \mathbb{Z}/m\mathbb{Z} \), then \( M \) is a finite abelian group of exponent \( m' \) which is a divisor of \( m \) and in case \( F = \mathbb{Q} \) then \( M \) is a finite dimensional vector space over \( \mathbb{Q} \). Given any subset \( A \) of \( M \) we write \( \langle A \rangle \) to denote the submodule of \( M \) spanned by \( A \). Notice that if \( F = \mathbb{Z}/m\mathbb{Z} \), then \( \langle A \rangle \) is same as the subgroup generated by \( A \), but if \( F = \mathbb{Q} \) then in general the subgroup generated by \( A \) is a proper subset of \( \langle A \rangle \). Given any finite subset \( C \) of \( M \), we set

\[
S(k_1, k_2, C, M) = \{ A \in S(k_1, k_2, M) : A \subset C \},
\]
and \( S^-(k_1, k_2, C, M) \) = \( \{ A \in S^-(k_1, k_2, M) : A \subset C \} \),
where \( S(k_1, k_2, M) \) and \( S^-(k_1, k_2, M) \) are as defined in (3) and (4) respectively.

For the purpose of obtaining an upper bound for clique number of random
Cayley sum graphs in a cyclic group of order \( n \), an upper bound for the
 cardinality of \( S(k_1, k_2, C, M) \) with \( M = F = \mathbb{Q} \) and \( C = \{0, 1, \ldots, n - 1\} \) was used by Green in [6].

**Freiman s-homomorphism:** Let \( s \) be a positive integer, let \( A \) and \( B \) be
subsets of (possibly different) abelian groups and let \( \phi : A \rightarrow B \) be a map.
Then we say that \( \phi \) is a Freiman \( s \)-homomorphism if whenever
\( a_1, \ldots, a_s, a'_1, \ldots, a'_s \in A \) satisfy
\[
a_1 + a_2 + \ldots + a_s = a'_1 + a'_2 + \ldots + a'_s
\]
we have
\[
\phi(a_1) + \phi(a_2) + \ldots + \phi(a_s) = \phi(a'_1) + \phi(a'_2) + \ldots + \phi(a'_s).
\]

If \( \phi \) has an inverse which is also \( s \)-homomorphism then we say that it is a
Freiman \( s \)-isomorphism. We shall refer to Freiman \( 2 \)-homomorphisms
simply as Freiman homomorphisms.

We shall obtain an upper bound for \( \text{card}(S(k_1, k_2, C, M)) \) by obtaining an
upper bound for the number \( c(k_1, k_2, C, M) \) of Freiman isomorphism classes
of sets in \( S(k_1, k_2, C, M) \) and an upper bound for the number \( n(A, C) \)
of subsets of \( C \) which are Freiman isomorphic to \( A \) for any given \( A \in S(k_1, k_2, C, G) \). Then we have
\[
\text{Card} (S(k_1, k_2, C, M)) \leq c(k_1, k_2, C, M) \max_{A \in S(k_1, k_2, C, M)} n(A, C). \tag{7}
\]

Using similar arguments we shall obtain an upper bound for \( \text{Card} (S^-(k_1, k_2, C, M)) \).

Let \( A \) be a subset of \( M \) with \( \text{card}(A) = k_1 \). Let \( e_1, e_2, \ldots, e_{k_1} \) be the
canonical basis of \( F^{k_1} \). We write \( R_s \) to denote the subset of \( F^{k_1} \) consisting
of the elements of the form
\[
e_{i_1} + e_{i_2} + \ldots + e_{i_s} - e_{j_1} - e_{j_2} - \ldots - e_{j_s},
\]
where \( i \)'s and \( j \)'s need not be distinct. For any subset \( A = \{a_1, a_2, \ldots, a_{k_1}\} \subset G \), let \( \phi : F^{k_1} \rightarrow G \) be the \( F \)-linear map with \( \phi(e_i) = a_i \). We write \( R_s(A) \) to
denote the set \( R_s \cap \ker(\phi) \). Let \( A_{r,s} = \{e_{i_1}, \ldots, e_{k_1}\} \) be the image of
\( \{e_1, e_2, \ldots, e_{k_1}\} \) in \( F^{k_1}/\langle R_s(A) \rangle \) under the natural projection map from \( F^{k_1} \) to \( F^{k_1}/\langle R_s(A) \rangle \). Then \( \phi \) induces a map \( \bar{\phi} : A_{r,s} \rightarrow A \).

**Lemma 7.** With the notations as above, the map \( \bar{\phi} : A_{r,s} \rightarrow A \) is a Freiman
\( s \)-isomorphism.
Proof. Since $\tilde{\phi}$ is a restriction of group homomorphism, it follows that it is a Freiman $s$-homomorphism. Moreover it is evident that $\tilde{\phi}$ is a bijective map. To prove that $\tilde{\phi}$ is a Freiman $s$-isomorphism we need to show that

$$
\tilde{\phi}(e_{i_1}) + \ldots + \tilde{\phi}(e_{i_s}) - \tilde{\phi}(e_{j_1}) - \ldots - \tilde{\phi}(e_{j_s}) = 0
$$

implies that

$$
e_{i_1} + \ldots + e_{i_s} - e_{j_1} - \ldots - e_{j_s} = 0.
$$

From (8), it follows that $e_{i_1} + \ldots + e_{i_s} - e_{j_1} - \ldots - e_{j_s} \in \ker(\phi) \cap R_s = R_s(A)$. Therefore it follows that (9) holds. Hence the lemma follows. \qed

1.1 Number of sets in a given Freiman $2$-isomorphism class

Given any $F$-modules $H$, $H'$ and a subset $B$ of $H'$, we write $Hom_s(B, H)$ to denote the space of Freiman $s$-isomorphism from $B$ into $H$. We also write $Hom_F(\langle B \rangle, H)$ to denote the space of $F$-linear map from $\langle B \rangle$ into $H$. Notice that $Hom_s(B, H)$ and $Hom_F(\langle B \rangle, H)$ are $F$-modules.

Lemma 8. Let $H$ be a $F$ module. Then any $g \in Hom_s(A_{r,s}, H)$ extends as a $F$-linear map $\tilde{g} : \langle A_{r,s} \rangle \rightarrow H$. The map thus obtained from $Hom_s(A_{r,s}, H)$ to $Hom_F(\langle A_{r,s} \rangle, H)$ is an isomorphism of modules.

Proof. Let $g \in Hom_s(A_{r,s}, H)$. Since $F^{k_1}$ is a free module and $e_i$'s are canonical basis of $F^{k_1}$ we have the following $F$-linear map $g' : F^{k_1} \rightarrow H$ with $g'(e_1) = g(e_1)$. Let $x \in R_s(A)$, then $x = e_{i_1} + e_{i_2} + \ldots + e_{i_s} - e_{j_1} - e_{j_2} - \ldots - e_{j_s}$. Then from the definition of $g'$ and the fact that $g$ is a Freiman $s$-homomorphism, it follows that $R_s(A) \subset \ker(g')$, implying that $\langle R_s(A) \rangle \subset \ker(g')$. Therefore we have the $F$-linear map $\tilde{g} : F^{k_1}/\langle R_s(A) \rangle \rightarrow H$ with $\tilde{g}(e_i) = g(e_i)$. Since $\langle A_{r,s} \rangle = F^{k_1}/\langle R_s(A) \rangle$, the map $\tilde{g}$ is an extension of $g$. Therefore we have a $F$-linear map $f : Hom_s(A_{r,s}, H) \rightarrow Hom_F(\langle A_{r,s} \rangle, H)$ with $f(g) = \tilde{g}$ for any $g \in Hom_s(A_{r,s}, H)$. It is evident that $f$ is injective. Moreover $f$ is surjective, since the restriction of any map in $Hom_F(\langle A_{r,s} \rangle, H)$ to $A_{r,s}$ is a Freiman $s$-homomorphism. Thus $f$ is an isomorphism of modules. \qed

Lemma 9. [6] Lemma 25] Let $H$ be a $F$-module. Then for any finite subset $B$ of $H$, there exists a subset $X$ of $B$ with $\text{card}(X) \leq \frac{4k_2 \log k_1}{k_1}$, where $k_1 = \text{card}(B)$ and $k_2$ is equal to $\min(\text{card}(B+B), \text{card}(B-B))$, such that $\langle X \rangle = \langle B \rangle$.

Proof. For any positive integer $l$, let $lB$ denotes the subset of $H$ consisting of those elements which can be written as a sum of $l$ elements of $H$. Since $\text{card}(B + B) \leq \text{card}(B+B) + \text{card}(B)$, using Plünette-Ruzsa inequality, we verify that for any positive integer $l$, we have

$$
\text{card}(lB) \leq \left(\frac{k_2 + k_1}{k_1}\right)^l.
$$

7
Let $\prec$ be an arbitrary ordering on $H$. Choose a subset $X$ of $B$ with the property that the sums $x_1 + x_2 + \cdots + x_l (x_1 \prec x_2 \prec \cdots \prec x_l)$ are all distinct, with $l = [\log_p k_1]$, and which is maximal with respect to this property. It follows from the definition of $X$ that $B \subset hX - (h-1)X$ and thus $\langle X \rangle = \langle B \rangle$. Moreover from the definition of $X$ we also have $\binom{\text{card}(X)}{l}$ is at most $\text{card}(IB)$. Using this we verify that $\text{card}(X) \leq \frac{4k_2 \log k_1}{k_1}$. Hence the lemma follows. \hfill $\square$

**Proposition 10.** Let $M$ be a $F$-module and $C$ is a finite subset of $M$. For any finite subset $A$ of $M$, the number of subsets of $C$ which are Freiman 2-isomorphic to $A$ is at most $\text{card}(C) \frac{4k_2 \log k_1}{k_1}$, where $k_1$ is equal to $\text{card}(A)$ and $k_2$ is equal to $\min \left( \text{card}(A+A), \text{card}(A-A) \right)$.

**Proof.** The number of subsets of $C$ which are Freiman 2-isomorphic to $A$ is at most the number of $g$ in $\text{Hom}_2(A, \langle C \rangle)$ with $g(A) \subset C$. Since $A$ and $A_{r,2}$ are Freiman 2-isomorphic, this number is at most the number of $g'$ in $\text{Hom}_2(A_{r,2}, \langle C \rangle)$ with $g'(A_{r,2}) \subset C$. Using Lemma 8 this is at most the number of $F$-linear map $\tilde{g}$ in $\text{Hom}_F(\langle A_{r,2} \rangle, \langle C \rangle)$ with $\tilde{g}(A_{r,2}) \subset C$. Using Lemma 8 we have that the module $\langle A_{r,2} \rangle$ is spanned by a subset $X$ of $A_{r,2}$ with $\text{card}(X) \leq \frac{4k_2 \log k_1}{k_1}$. Since $\tilde{g}$ is uniquely determined by its value on $X$, the number of such $\tilde{g}$ is at most $\text{card}(C) \frac{4k_2 \log k_1}{k_1}$. Hence the proposition follows. \hfill $\square$

### 1.2 Number of Freiman isomorphism classes

We set $g(F)$ to be equal to 1 in case $F$ is a field and to be equal to the number of distinct prime divisors of $m$, when $F = \mathbb{Z}/m\mathbb{Z}$. We shall need the following lemma.

**Lemma 11.** For any subset $R$ of $F^k$, there exists a subset $R_0$ of $R$ with $\text{card}(R_0) \leq g(F)k$ such that $\langle R_0 \rangle = \langle R \rangle$.

**Proof.** When $F$ is a field, the dimension of the subspace $\langle R \rangle$ of $F^k$ is at most $k$ and there exists a subset $R_0$ of $R$ which forms a basis of the vector space $\langle R \rangle$. Thus the lemma follows in this case.

Now we need to prove the lemma in case when $F = \mathbb{Z}/m\mathbb{Z}$. In this case we shall prove the lemma by an induction on $k$.

We first prove the lemma in case $k = 1$. In this case $\langle R \rangle$ is equal to a subgroup of $\mathbb{Z}/m\mathbb{Z}$. Let $p : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ be the natural projection map and for any $x \in \mathbb{Z}/m\mathbb{Z}$, we write $\bar{x}$ to denote the integer in $[0, m-1]$ with $p(\bar{x}) = x$.

If the order of $\langle R \rangle$ is $d$, then $p^{-1}(\langle R \rangle) = \frac{m}{d} \mathbb{Z}$. Thus for any prime divisor $p$ of $m$, there exists $r_p \in R$ such that $\bar{r_p} = \frac{m}{d} r'_p$ with $p$ not dividing $r'_p$. Let $R_0 = \{ r_p \}_{p|m}$. We claim that $\langle R_0 \rangle = \langle R \rangle$.

Suppose the claim is not true. Then $\langle R_0 \rangle$ is a proper subgroup of $\langle R \rangle$ and there exists a positive integer $d'$ which divides $m$ such that $p^{-1}(\langle R_0 \rangle)$
Figure 9

consists of those integers which are divisible by \( \frac{m}{d}d' \). But by construction of \( R_0 \) we have that for any prime \( p|d' \) we verify that \( \tilde{r}_p \) is not divisible by \( \frac{m}{d}d' \). This contradiction proves the claim and \( \langle R_0 \rangle = \langle R \rangle \). Moreover by the construction of the \( R_0 \), we have \( \text{card}(R_0) \leq \omega(m) \). Hence the lemma follows in case \( k = 1 \).

Now suppose the lemma is true for any \( k \leq l - 1 \) with \( l \geq 2 \). We shall show that the lemma holds for \( k = l \). Let \( \pi_1 : F^l \rightarrow F \) be the projection map on the first co-ordinate. Then \( \pi_1((R)) \) is the module of \( F \) and using the fact that the lemma holds for \( k = 1 \), it follows that there exist \( R_0' \subset R \) with \( \text{card}(R_0') \leq g(F) \) such that \( \pi_1((R_0')) = \pi_1((R)) \). Thus for any \( r \in R \), there exist \( r_1 \in \langle R_0' \rangle \) such that \( \pi(r - r_1) = 0 \). Let \( \tilde{r}'' = \{r - r_1 : r \in R \} \). Then \( \tilde{r}'' \subset F^{l-1} \) and by the induction hypothesis there exist a subset \( R_0'' \) of \( R'' \) such that \( \text{card}(R_0'') \leq g(F)(k - 1) \) and \( \langle R'' \rangle = \langle R_0'' \rangle \). Let \( R_0 = R_0' \cup R_0'' \). Since \( \langle R \rangle = \langle R'' \rangle + \langle R_0' \rangle \), it follows that \( \langle R_0 \rangle = \langle R \rangle \). Moreover we have that \( \text{card}(R_0) \leq \text{card}(R_0') + \text{card}(R_0'') \leq g(F)k \). Hence the lemma follows.

The following lemma is a generalisation of [[6], Lemma 11].

**Lemma 12.** Let \( H \) be an \( F \)-module. Then the number of Freiman \( s \)-isomorphism classes of subsets of \( H \) of the cardinality \( k \) is at most \( k^{2^g(F)k} \).

**Proof.** Let \( c(k) \) be the number of Freiman \( s \)-isomorphism classes of subsets of \( H \) of the cardinality \( k \). From Lemma 7 any subset \( B \) of the cardinality \( k \) is isomorphic to \( B_{r,s} \), which is the image of canonical basis of \( F^k \) under the projection map from \( F^k \) to \( F^k/\langle R_s(B) \rangle \) where \( R_s(B) \) is a subset of \( R \). Thus \( c(k) \) is at most the number of submodules of \( F^k \) which are spanned by a subset of \( R_s \). Using Lemma 11 any such submodule is spanned by a subset \( R_0 \) of \( R_s \) of cardinality at most \( g(F)k \). Thus \( c(k) \leq \sum_{i=0}^{g(F)k} \binom{k^2}{i} \leq k^{2^g(F)k} \).

Using Lemma 7 the Freiman \( s \)-isomorphism class of any subset \( A \) of an \( F \)-module \( H \) is determined by \( s \)-relation satisfied by it. Using this and the arguments used in the proof of [[6], Lemma 16], we obtain the following result.

**Lemma 13.** [[6], Lemma 16] Let \( H \) be an \( F \)-module. Fix a non-negative integer \( t \) and a subset \( B \) of \( M \) with \( \text{card}(B) = l \). Then the number of mutually non-isomorphic sets \( A \) with \( \text{card}(A) = l + t \), such that there exists a subset \( A_0 \subset A \) satisfying \( A_0 \) is Freiman \( 3 \)-isomorphic to \( B \) is at most \((l^3 + 1)^{d^4}\).

For any subset \( A \) of an \( F \)-module \( H \), let \( A_0 \) be a subset of \( A \) of the minimum possible cardinality among the subsets of \( A \) satisfying the property that there exists \( a^* \in A \) such that \( a^* + (A \setminus \{a^*\}) \subset A_0 \wedge A_0 \). Among all the possible choices of \( A_0 \), we choose the one with the minimum possible cardinality of \( A_0 \wedge A_0 \). For any positive integers \( s_1, s_2 \), we define the following subset of \( S(k_1, k_2, C, M) \).

\[
S(k_1, k_2, s_1, s_2, C, M) = \{ A \in S(k_1, k_2, C, M) : \text{card}(A_0) = s_1, \text{card}(A_0 \wedge A_0) = s_2 \}.
\]

(10)
For any \( A \in S^-(k_1, k_2, C, M) \), we also choose a subset \( A_0 \) of \( A \) which is of the minimum possible cardinality among the subsets of \( A \), satisfying that there exist an \( a^* \in A \) such that \( a^* - A \subset A_0 - A_0 \). Among all the possible choices of \( A_0 \) we choose a one with the cardinality of \( A_0 - A_0 \) minimal possible. For any positive integers \( s_1 \) and \( s_2 \) we set

\[
S^-(k_1, k_2, s_1, s_2, C, M) = \{ A \in S^-(k_1, k_2, C, M) : \text{card}(A_0) = s_1, \text{card}(A_0 - A_0) = s_2 \}.
\]

The following lemma is an easy exercise.

**Lemma 14.** [8 Lemma 16] Suppose that \( X \cong_0 X' \). Then \( X + X \cong_3 X' + X' \) and any subset \( B \subset X + X \) is 3-isomorphic to a subset of \( X' + X' \). Similarly \( X - X \cong_3 X' - X' \) and any subset \( B \) of \( X - X \) is Freiman 3-isomorphic to a subset of \( X' - X' \).

Using Lemmas 12, 13, 14 and the argument used in the proof of [6 Proposition 18] we obtain the following result.

**Proposition 15.** Let \( M \) be an \( F \)-module. Then the number of Freiman 2-isomorphism classes of sets in \( S(k_1, k_2, s_1, s_2, C, M) \) as well as in \( S^-(k_1, k_2, s_1, s_2, C, M) \) is at most \( (s_1)^{12\sigma(F)}s_1(k_1^3 + 1) \).

Now we obtain an upper bound for the cardinality of \( A_0 \) for any \( A \in S(k_1, k_2, C, M) \).

**Lemma 16.** For any \( A \in S(k_1, k_2, C, M) \), there exist \( a^* \in A \), \( A_0' \subset A \) and \( A_1 \subset A \) with \( \text{card}(A_0') + \text{card}(A \setminus A_1) \ll (k_1k_2 \log k_1)^{1/3} \) such that \( a^* + A_1 \subset A_0' + A_0' \). Similarly for any \( A \in S^-(k_1, k_2, C, M) \), there exist \( a^* \in A \), \( A_0' \subset A \) and \( A_1 \subset A \) with \( \text{card}(A_0') + \text{card}(A \setminus A_1) \ll (k_1k_2 \log k_1)^{1/3} \) such that \( a^* - A_1 \subset A_0' - A_0' \).

**Proof.** The proof follows from the arguments used in the proof of [6 Proposition 15] with the choice of the parameters \( Q \) to be \( \left[ \frac{k_1^{4/3}}{k_2^{2/3}} \log^{1/3} k_1 \right] \) and \( q \) to be \( 100^{1/3}/k_2^{1/2} \sqrt{Q} \). In [6 Proposition 15] it was assumed that \( k_2 \leq k_1^{31/30} \) and the choice of parameters \( Q \) and \( q \) used were \( [k_1^{1/5}] \) and \( k_1^{-1/15} \) respectively. \( \square \)

**Corollary 17.** For any \( A \in S(k_1, k_2, C, M) \), let \( A_0 \) be a subset of \( A \) as define above. Then we have \( \text{card}(A_0) \ll (k_1k_2 \log k_1)^{1/3} \). Similar statement holds for any \( A \in S^-(k_1, k_2, C, M) \).

**Proof.** For any \( A \in S(k_1, k_2, C, M) \), let \( A_1, A_0' \) be subsets of \( A \) as provided by the previous lemma. We take \( A_0'' = A_0' \cup \{a^*\} \cup (A \setminus A_1) \). Then it follows that \( a^* + (A \setminus \{a^*\}) \subset A_0'' + A_0'' \) and \( \text{card}(A_0'') \ll (k_1k_2 \log k_1)^{1/3} \). This proves the claim for any \( A \in S(k_1, k_2, C, M) \). Similar arguments prove the claim for any \( A \in S^-(k_1, k_2, C, M) \). \( \square \)
2 Proof of Theorems 6 and 3

Proof of Theorem 6. Using Proposition 13, Lemmas 17 and 12 with $F = \mathbb{Z}/m\mathbb{Z}$ and $M = C = G$, it follows that there exist an absolute constant $c > 0$ such that the number of Freiman isomorphism classes of sets in $S(k_1, k_2, G)$ is at most

$$\min \left( k_1^{\omega(n)(k_1 k_2 \log k_1)^{1/3}} \left( \frac{k_2}{k_1 - 1} \right)^{(k_1^3 + 1), k_1^4 k_1} \right).$$

For obtaining the above estimate we have also used the fact that $\text{card}(A_0 + A_0) \leq k_2$ and since $m$ is the exponent of $G$, we have $\omega(m) = \omega(n)$. Similar arguments show that the same upper bound holds for the number of Freiman isomorphism classes of sets in $S^-(k_1, k_2, G)$. Then the theorem follows using (7) and Proposition 10 with $C = M = G$. \hfill \Box

Proof of Theorem 3. For any $A \in S^-(k_1, k_2, G)$, let $A_0$ be a subset of $A$ as defined above. Since $\alpha^* - A \subset A_0 - A_0$, we have $\text{card}(A_0 - A_0) \geq k_1$. Moreover from Lemma 17 we have that $\text{card}(A_0) \ll (k_1 k_2 \log k_1)^{1/3}$. Thus if $k_1$ is sufficiently large, then there exists a subset $A'$ of $G$ with $A_0 \subset A' \subset A$ such that we have $\text{card}(A') \geq \frac{k_1}{100}$ and $\text{card}(A' - A') \geq 100 \text{card}(A')$. Now if $A$ spans a complete subgraph in a random Cayley graph $G_B$ then so does $A'$. Therefore we obtain

$$\mathbb{P}(\text{cl}(B) \geq k_1) \leq \sum_{k_1/100 \leq k'_2 \leq k_1, k'_2 \geq 100k'_1} \frac{\text{card}(S(k'_1, k'_2, G))}{2(k'_2 - 1)/2}. \quad (11)$$

Then using Theorem 6 we verify the following inequality.

$$\mathbb{P}(\text{cl}(B) \geq k_1) \leq \sum_{k_1/100 \leq k'_1 \leq k_1, k'_2 \geq 100k'_1} 2^{-k'_2 g(k'_1, k'_2, n)}, \quad (12)$$

with

$$g(k'_1, k'_2, n) = -\frac{\omega(n)(k'_1 \log k'_1)^{1/3} \log k'_1}{k'_2^{2/3}} - \frac{1}{k'_2 \log \left( \frac{k'_2}{k'_1 - 1} \right)} - \frac{4 \log k'_1 \log n}{k'_1} + 1/2 - \frac{1}{2k'_2}.$$

Since $k'_2 \geq 100k'_1$, using the inequality $\left( \frac{k'_2}{k'_1} \right)^{k'_1} \leq \left( \frac{e k'_1}{n} \right)^{k'_1}$, it follows that there exist an absolute constant $c_1$ such that for $k'_1 \geq c_1 (\omega^3(n) \log \omega(n) + \log n \log \log n)$, then $g(k'_1, k'_2, n) \geq c_2$, for some absolute constant $c_2 > 0$. Using this and (12), the theorem follows. \hfill \Box

3 Freiman rank of a set

In this section we prove Corollary 24 which was proven by Ben Green in 6, Corollary 14] in the case when $F$ is a field. Although the result is not
required for proving other results of this article, it may be of an independent interest.

**Rank of an F-module:** For any F-module H, the rank of H is the least non negative integer r(H) such that there is a surjective F-linear map from \( F^{r(H)} \) to H.

**Freiman s-rank:** Given any finite subset B of a F module H and a positive integer s, we define Freiman s-rank \( r_s(B) \) to be \( r(\text{Hom}_s(B, F)) - 1 \). In case F is a field and \( s = 2, r_s(B) \) is the Freiman dimension of B as defined by Ben Green in [6].

We will need the following well known fact.

**Lemma 18.** Let \( F \) be either equal to \( \mathbb{Z}/m\mathbb{Z} \) or is equal to \( \mathbb{Q} \). For any finitely generated F-module H, the dual module \( \text{Hom}_F(H, F) \) is isomorphic to H.

**Lemma 19.** \( r_s(A) = r_s(A_{r,s}) = r(\langle A_{r,s} \rangle) - 1 \).

**Proof.** Since \( A \) and \( A_{r,s} \) are Freiman s-isomorphic, the first equality follows. From Lemma 8 the module \( \text{Hom}_s(A_{r,s}, F) \) is isomorphic to the module \( \text{Hom}_F(\langle A_{r,s} \rangle, F) \), which from Lemma 18 is isomorphic to \( \langle A_{r,s} \rangle \). Hence the second equality follows.

**Lemma 20.** There exists a unique F-linear map \( \phi_0 : \langle A_{r,s} \rangle \rightarrow F \) with \( \phi_0(x) = 1_F \) for any \( x \in A_{r,s} \). In case \( F = \mathbb{Z}/m\mathbb{Z} \), and hence \( \langle A_{r,s} \rangle \) is a finite abelian group, the order of any element in \( A_{r,s} \) is equal to m.

**Proof.** The constant map \( \phi'_0 : A_{r,s} \rightarrow F \) with \( \phi'_0(x) = 1_F \) for any \( x \in A_{r,s} \) is a Freiman s-homomorphism. Therefore using Lemma 8 there exists a unique F-linear map \( \phi_0 : \langle A_{r,s} \rangle \rightarrow F \) with \( \phi_0(x) = 1_F \) for any \( x \in A_{r,s} \). This proves the first part of the lemma. In case \( F = \mathbb{Z}/m\mathbb{Z} \), let \( x \) be any fixed element in \( A_{r,s} \) and \( d \) be the order of \( x \). Since \( \phi_0 \) is F-linear, it follows that \( \phi_0(dx) = d\phi_0(x) = 0 \). Since \( \phi_0(x) = 1_F \), it follows that \( d = m \).

**Lemma 21.** Let \( H \) be a finitely generated F-module. In case \( F = \mathbb{Z}/m\mathbb{Z} \) and hence \( H \) is a finite abelian group, then \( H = \bigoplus_{i=1}^r A_i \), where \( r = r(H) \) and \( A_i \)'s are cyclic groups. Moreover given any element \( x_1 \in H \) with order of \( x_1 \) being equal to the exponent of \( H \), there exist \( A_i \)'s as above with \( A_1 = \langle x_1 \rangle \).

**Proof.** From the structure theorem of finite abelian groups, we have that \( H = \bigoplus_{i=1}^r A_i \), where \( s \) is a positive integer and \( A_i \)'s are cyclic groups isomorphic to \( \mathbb{Z}/c_i\mathbb{Z} \) with \( c_i | c_{i-1} \) for all \( 2 \leq i \leq s \). Moreover going through the proof of [7] Theorem 2.14.1] the last claim of the lemma follows. To prove the lemma we need to show that \( s = r \). A subset of \( H \) containing an element \( x_i \) from each \( A_i \) with \( x_i \) being a generator of \( A_i \) is of cardinality \( s \) and spans \( H \) as an F-module. Thus from the definition of the rank of an F-module we have \( r \leq s \).
Moreover using the definition of a rank of an $F$-module we have a surjective group homomorphism $f : \mathbb{Z}^r \to H$. Since $\mathbb{Z}^r$ is a free module over the principle ideal domain $\mathbb{Z}$, we have that $\ker(f)$ is also a free module over $\mathbb{Z}$. Moreover there exist a basis $\{y_1, \ldots, y_r\}$ of $\mathbb{Z}^r$ such that the basis of $\ker(f)$ is $\{u_1y_1, \ldots, u ry_r\}$, where $u_i$'s are positive integers. Thus $\mathbb{Z}^r / \ker(f) = \bigoplus_{i=1}^{r} \mathbb{Z}/u_i \mathbb{Z}$. Since $H$ is isomorphic to $\mathbb{Z}^r / \ker(f)$ it follows that $H$ can be written as a direct sum of $r$ cyclic groups. But we also have that $H$ is isomorphic to $\bigoplus_{i=1}^{s} \mathbb{Z}/c_i \mathbb{Z}$ with $c_i | c_{i-1}$ for any $i$ which satisfies $2 \leq i \leq s$. The condition that $c_i | c_{i-1}$ implies that $s$ is the least positive integer $d$ such that $H$ can be written as a direct sum of $d$ cyclic groups. Therefore we have

$$s \leq r. \quad (14)$$

Combining (13) and (14) we have $s = r$. Hence the lemma is proven. \hfill \square

**Lemma 22.** There exists a subset $X = \{x_1, \ldots, x_r\}$ of $\langle A_{r,s} \rangle$ of cardinality $r = r(\langle A_{r,s} \rangle)$ such that $x_1 \in A_{r,s}$ and $\langle X \rangle = \langle A_{r,s} \rangle$.

**Proof.** In case $F$ is a field, we have a subset $X$ of $A_{r,s}$ such that $X$ forms a basis of the vector space $\langle A_{r,s} \rangle$. Thus the claim follows in this case. In case $F = \mathbb{Z}/m\mathbb{Z}$, then from Lemma 20 the order of any element in $A_{r,s}$ is equal to the exponent of $H$. Then using Lemma 21 we have that $\langle A_{r,s} \rangle = \bigoplus_{i=1}^{r} A_i$ with $A_i = \langle x_i \rangle$ and $x_1 \in A_{r,s}$. Therefore $X = \{x_1, \ldots, x_r\}$ is a subset of $\langle A_{r,s} \rangle$ satisfying the assertion of the lemma. \hfill \square

**Proposition 23.** Let $A_{r,s} = \{\bar{e}_1, \ldots, \bar{e}_{k_1}\}$ be as above. Then the rank of the submodule $H_A = \langle \bar{e}_2 - \bar{e}_1, \ldots, \bar{e}_{k_1} - \bar{e}_1 \rangle$ of $\langle A_{r,s} \rangle$ is equal to $r_s(A) = r(\langle A_{r,s} \rangle) - 1$.

**Proof.** Since $A_{r,s}$ is contained in $H_A + \bar{e}_1$ and from Lemma 19 the rank of $\langle A_{r,s} \rangle$ is equal to $r_s(A) + 1$, it follows that $r(H_A) \geq r_s(A)$. For proving the lemma we shall show that $H_A$ is contained in a module $H$ of rank at most $r_s(A)$. Let $X = \{x_1, \ldots, x_r\}$ be a subset of $A_{r,s}$ with $x_1 = \bar{e}_1$ and $r = r_s(A) + 1$ as provided by Lemma 22. Since $\langle X \rangle = \langle A_{r,s} \rangle$, for any $i$ with $1 \leq i \leq k_1$, there exists $\lambda_{j,i} \in F$ such that

$$\bar{e}_i = \sum_{j=1}^{r} \lambda_{j,i} x_j. \quad (15)$$

Let $\phi_0$ be the $F$-linear map as in Lemma 20. Then evaluating the value of the both sides of the above equality for the map $\phi_0$, we obtain that

$$1_F = \sum_{j=1}^{r} \lambda_{j,i} \phi_0(x_j).$$

Moreover since $x_1 = \bar{e}_1$ and thus $\phi_0(x_1) = \phi_0(\bar{e}_1) = 1_F$, it follows that for any $i$, we have $\lambda_{1,i} = 1 - \sum_{j=2}^{r} \phi_0(x_j)$. Using this and (15) it follows that $A_{r,s} \subset x_1 + H$ where $H$ is the module $\langle x_2 - \phi_0(x_1)x_1, \ldots, x_r - \phi_0(x_r)x_1 \rangle$. Thus $H$ contains $H_A$ and its rank is clearly less than or equal to $r - 1$. Therefore it follows that $r(H_A) \leq r - 1 = r_s(A)$. Hence the lemma follows. \hfill \square
Corollary 24. Let \( A \) be a finite subset of an \( F \)-module \( H \). Then \( r_s(A) \) is the largest integer \( d \) such that \( A \) is Freiman \( s \)-isomorphic to a subset \( X \) of a module \( H \) of rank \( d \) and \( X \) is not contained in a translate of any proper submodule of \( H \).

Proof. From Lemma 19 we have \( r_s(A) = r_s(A_{r,s}) \). Let \( B = \{ 0, \bar{e}_2 - \bar{e}_1, \ldots, \bar{e}_k - \bar{e}_1 \} \). Then we have a Freiman \( s \)-isomorphism \( f : A_{r,s} \to B \) defined by \( f(\bar{e}_i) = \bar{e}_i - \bar{e}_1 \). From Proposition 23 the rank of the module \( \langle B \rangle = H_A \) is equal to \( r_s(A) \). Moreover we observe that if \( B \) is contained in \( H' + x \) for some submodule \( H' \) of \( H \), then since \( B \) contains 0, it follows that \( x \in H' \) and \( H' = H_A = \langle B \rangle \). In other words \( B \) is not contained in a translate of any proper submodule of \( \langle B \rangle \). This implies that \( d \geq r_s(A) \).

Now using Lemma 8 any Freiman \( s \)-isomorphism \( f : A_{r,s} \to X \) extends as a \( F \)-linear map \( \tilde{f} : \langle A_{r,s} \rangle \to \langle X \rangle \). Since \( A_{r,s} \subset H_A + \bar{e}_1 \), we have that \( X \subset \tilde{f}(H_A) + \tilde{f}(\bar{e}_1) \). Since the rank of \( \tilde{f}(H_A) \) is at most the rank of \( H_A \) which is equal to \( r_s(A) \), it follows that any set isomorphic to \( A \) is contained in a translate of a module of rank at most \( r_s(A) \). This implies that \( d \leq r_s(A) \). Hence \( r_s(A) = d \).

4 Concluding remarks

A subset \( A \) of an abelian group \( G \) is said to be sum-free if there is no solution of the equation \( x + y = z \) with \( x, y, z \in A \). In [3] it was shown that the problem of obtaining an upper bound for the number of sum-free sets in certain types of finite abelian groups is equivalent to obtaining an upper bound for

\[
a(H) = \sum_{k_1,k_2} \frac{\text{Card}(S(k_1,k_2,H))}{2^{k_2}},
\]

with \( H = G/(\mathbb{Z}/m\mathbb{Z}) \), where \( m \) is the exponent of \( G \). Using the upper bound for \( \text{card}(S(k_1,k_2,H)) \) provided by Theorem 6 it follows that

\[
a(H) \leq n^{2/3 \log n},
\]

where \( n \) is the order of \( H \). One could also show that

\[
a(H) \geq \frac{s(H)}{2},
\]

where \( s(H) \) is the number of subgroups of \( H \). Using Theorem 6 one may verify that the main contribution in the right hand side of (16) comes from those summands with \( (2 - \epsilon)k_1 \leq k_2 \leq (2 + \epsilon)k_1 \).

Acknowledgement

I thank R. Balasubramanian, D.S. Ramana for many helpful discussions and carefully reading the manuscript. I would also like to thank Jean-Marc Deshouillers, Imre Ruzsa and Gilles Zémor for making several useful comments. A part of this work was done when I was a post doctoral fellow at Harish-Chandra research institute (HRI), Allahabad, India. I am grateful for the support I received during my stay at HRI.
References

[1] N. Alon. Graph powers. In Contemporary Combinatorics, volume 10 of Bolyai Math. Soc. Stud., pages 11–28. Springer, 2002.

[2] N. Alon and A. Orlitsky. Repeated communications and Ramsey graphs. IEEE Transactions on Information Theory, 41:1276–1289, 1995.

[3] R. Balasubramanian, Gyan Prakash, and D.S. Ramana. Sum-free subsets of finite abelian groups of type III. http://arxiv.org/abs/0711.4317.

[4] B. Bollobas. Random Graphs, volume 73. Cambridge studies in advanced mathematics, second edition, 2001.

[5] F. R. K. Chung. A note on constructive methods for Ramsey numbers. J. Graph Theory, 5:109–113, 1981.

[6] Ben Green. Counting sets with small sumset, and the clique number of random Cayley graphs. Combinatorica, 25(3):307–326, 2005.

[7] I.N. Herstein. Topics in Algebra. Wiley Eastern Limited, 2nd edition, 1975.

[8] Paul Erdős. Some remarks on the theory of graphs. Bull. Amer. Math. Soc., 53:292–294, 1947.

Institute of Mathematical Sciences,
CIT Campus, Taramani,
Chennai-600113,
India
gyan.jp@gmail.com