Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 79 (2004)

Artikel: A new critical pair theorem applied to sum-free sets in Abelian groups
Autor: Hamidoune, Yahya ould / Plagne, Alain
DOI: https://doi.org/10.5169/seals-59504

Comment. Math. Helv. 79 (2004) 183–207
0010-2571/04/010183-25
DOI 10.1007/s00014-003-0786-5

Commentarii Mathematici Helvetici

A new critical pair theorem applied to sum-free sets in Abelian groups

Yahya ould Hamidoune and Alain Plagne*

Abstract. We shall prove a new generalization of Vosper critical pair theorem to finite Abelian groups. We next apply this new tool to the theory of (k,l)-free sets in finite Abelian groups. In particular, in most cases, we describe the structure of maximal (k,l)-free sets and determine the maximal cardinality of such a set. This result allows us for instance to give precisions on an old result of Yap: we are able to describe completely the maximal sum-free sets with cardinality at least one third of that of the ambient group.

Mathematics Subject Classification (2000). 11P70, 20D60, 20K01, 11B25.

Keywords. Additive number theory, Vosper theorem, (k,l)-free sets, structure theorem.

1. Introduction

Two centuries ago, Cauchy proved the first result of what is called set addition theory [4]. We refer the reader to one of the accounts [18, 19] for the usual definitions and notations in this context. Translated into modern language, Cauchy's result reads as follows: let $\mathcal{A}$ and $\mathcal{B}$ be two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$ (p prime) then

$$|\mathcal{A}+\mathcal{B}| \geq \min(p, |\mathcal{A}|+|\mathcal{B}|-1).$$

This result was rediscovered more than a hundred years later by Davenport [5, 6] and is now known as the Cauchy–Davenport theorem. Vosper [26, 27] could characterize precisely the pairs of sets $(\mathcal{A},\mathcal{B})$ for which the Cauchy–Davenport inequality is in fact an equality (such pairs are said to be *critical*). To be more precise, the essential part of Vosper's theorem states that in $\mathbb{Z}/p\mathbb{Z}$, for any pair of sets $\mathcal{A},\mathcal{B}$ with $|\mathcal{A}|, |\mathcal{B}| \geq 2$, the relation

$$p-2 \geq |\mathcal{A}+\mathcal{B}| = |\mathcal{A}|+|\mathcal{B}|-1$$

can hold only if $\mathcal{A}$ is an arithmetic progression.

* Supported by the DGA-Recherche (France).

We know now several generalizations of Vosper's theorem to Abelian groups. The first one is a difficult but nice theory developed by Kemperman [15]. One of the authors [10, 11] also proposed generalizations using the isoperimetric method, a method introduced in [8, 9, 10]. In particular, the following result was obtained in [11] (as Theorem 6.6; but notice that there is a misprint in [11]: $|H|+|B|-1$ should be replaced by $|H|+|B|$ in case (iii) of Theorem 6.6).

Theorem A [11, 12]. *Let $\mathcal{A}$ be a generating subset of a finite Abelian group G such that $0\in\mathcal{A}$ and $|\mathcal{A}|\le|G|/2$, then one of the following conditions holds:*
(i) *$\mathcal{A}$ is an arithmetic progression,*
(ii) *there is a subgroup $H\neq\{0\}$ such that $|H+\mathcal{A}|<\min(|G|-1,|H|+|\mathcal{A}|)$,*
(iii) *for any $\mathcal{X}\subset G$ such that $|\mathcal{X}|\ge 2$,*

$$|\mathcal{A}+\mathcal{X}|\ge\min(|G|-1,|\mathcal{A}|+|\mathcal{X}|).$$

This result is useful in the study of several questions, including the Diophantine Frobenius problem or Freiman's $3k-3$ theorem (for instance, in [12], it was used as Lemma 2).

Vosper's result has several applications, including the characterization of maximal sum-free sets. Given two different positive integers k and l and an additively written group G, we say that a subset $\mathcal{S}$ of G is a *(k,l)-free set* (some authors use the terminologies *(k,l)-sum-free set* or simply *(k,l)-set*) if

$$k\mathcal{S}\cap l\mathcal{S}=\emptyset.$$

This holds if and only if $0\notin k\mathcal{S}-l\mathcal{S}$. Clearly, there is no restriction in assuming $k>l$. With the preceding definition, the *sum-free sets* coincide with the $(2,1)$-free sets. Sum-free sets have attracted a considerable amount of work (see for example [1] or the recent [3, 17]) and have been studied in various structures (natural integers, semi-groups, groups) and from many viewpoints (maximal cardinality, number, structure).

In the study of (k,l)-free sets in groups, the fundamental problem is, an arbitrary group G being given, the construction of all (k,l)-free sets of G. One may achieve this goal by describing the maximal (with respect to the inclusion) (k,l)-free sets in G. Two basic questions in this direction are the following:

– first, determine the maximal cardinality (denoted thereafter by $\lambda_{k,l}(G)$) of a (k,l)-free set in G, or at least improve on the trivial estimate

$$\lambda_{k,l}(G)\le\frac{|G|}{2},\qquad(1)$$

– second, describe such a (k,l)-free set having cardinality $\lambda_{k,l}(G)$.

We insist on the fact that, in this paper, a (k,l)-free set will be said to be *maximal* if it is maximal in the sense of inclusion. Although this remark looks quite evident, it is definitely worth mentioning it since in the first papers (by Yap and Diananda who together initiated the subject of sum-free sets in Abelian groups), maximal sets only means sets with maximal cardinality. During the seventies, sum-free sets with maximal cardinality in general finite Abelian groups have been widely studied (see for example the general account [28, Chapter 2]), motivated by the following conjecture essentially due to Yap.

Conjecture B. *Let G be a finite Abelian group, then*

$$\lambda_{2,1}(G) = \max_{d \mid \exp(G)} \left\{ \frac{[(d-2)/3]+1}{d} \right\} |G|.$$

This conjecture is tantamount to saying that, given an arbitrary Abelian group G, the value $\lambda_{2,1}(G)$ is attained for an arithmetic progression of H-cosets, where H is a subgroup of G such that the quotient group G/H is cyclic (see Lemma 5.2 below).

Conjecture B could be proved in any case except that of groups, whose cardinality is equal to a product of primes congruent to 1 modulo 3. In particular, the following result was obtained, not only but essentially, by Diananda and Yap. We recall that the *exponent* of a group G is the smallest integer n, denoted by $\exp G$, such that $nx = 0$ for all x in G (in additive notation).

Theorem C [7, 29, 30, 31, 32, 33, 34, 35]. *Let G be any finite Abelian group. There are three possible cases:*

(i) *if $|G|$ has at least one prime factor congruent to 2 modulo 3 then*

$$\lambda_{2,1}(G) = \frac{q+1}{3q}|G|,$$

where q is the smallest prime factor of $|G|$ congruent to 2 modulo 3,

(ii) *if $|G|$ has no prime factor congruent to 2 modulo 3 but 3 divides $|G|$ then*

$$\lambda_{2,1}(G) = \frac{|G|}{3},$$

(iii) *otherwise (that is, if any prime factor of $|G|$ is congruent to 1 modulo 3), denoting by m the exponent of G,*

$$\frac{m-1}{3m}|G| \leq \lambda_{2,1}(G) \leq \frac{|G|-1}{3}.$$

In the last case, Conjecture B is tantamount to saying that the lower bound is in fact an equality. This has been established in some special cases only (see [22, 35]).

Concerning the structural characterization of sum-free sets attaining the maximal cardinality $\lambda_{2,1}(G)$, it is known in case (i) and (ii) of Theorem A but not in case (iii). These results were obtained in Yap's papers and also in [22, 24, 25]. We shall not enunciate these results here. The reader is referred to Theorems 7.8 and 7.9 in [28, Part 3] where these results are precisely stated.

The question of (k,l)-free sets ($k \neq l$) in general finite Abelian groups has been less studied. Only the case of (k,l)-free subsets of $\mathbb{Z}/p\mathbb{Z}$ (p prime) is answered. In that case, both the value [2] of $\lambda_{k,l}(\mathbb{Z}/p\mathbb{Z})$ and the structure [21] of the (k,l)-free subsets of $\mathbb{Z}/p\mathbb{Z}$ with that cardinality are known.

Theorem D [2, 21]. *Let p be an odd prime and let k,l be positive integers not congruent modulo p and which satisfy* $\max(k,l) \geq 3$. *Then*

$$\lambda_{k,l}(\mathbb{Z}/p\mathbb{Z}) = \left\lceil \frac{p-1}{k+l} \right\rceil$$

and any (k,l)-free set with this maximal cardinality in $\mathbb{Z}/p\mathbb{Z}$ is an arithmetic progression.

The traditional approach in the study of sum-free sets in groups is via the use of Kneser's [16], Vosper's [26, 27] and Kemperman's [15] theorems. Theorem B deals with any k and l but it requires additional specific properties of $\mathbb{Z}/p\mathbb{Z}$ (the Cauchy–Davenport, Vosper and Hamidoune–Rødseth [14] theorems are used).

2. Main results

In this paper, we will first obtain yet another generalization of Vosper's theorem which is valid in any finite Abelian group (Theorem 2.1, proved in Section 3) and which is easy to apply.

To formulate our addition theorem, we need some notations. Let G be an arbitrary Abelian group and H a subgroup of G. We denote by $\psi_{G,G/H}$ the canonical homomorphism from G onto G/H. If $\mathcal{A}$ is any subset of G, it will be convenient to denote by $\mathcal{A}/H$ the subset $\psi_{G,G/H}(\mathcal{A})$ of G/H. In reference to Vosper's result, we say that a subset $\mathcal{A} \subset G$ is a *Vosper subset* of G if for any $\mathcal{X} \subset G$, with $|\mathcal{X}| \geq 2$,

$$|\mathcal{A} + \mathcal{X}| \geq \min(|G| - 1, |\mathcal{A}| + |\mathcal{X}|).$$

Let us finally recall that an *arithmetic progression* P in G is a set such that there are two elements a and d in G and a non-negative integer s with $P = \{a + jd | 1 \leq j \leq s\}$.

Here is our generalization of Vosper's theorem. To deduce Vosper's theorem from this result is left to the reader as an exercise.

Theorem 2.1. *Let $\mathcal{A}$ be a generating subset of a finite Abelian group G such that $0 \in \mathcal{A}$. Suppose also*

$$|\mathcal{A}| \leq |G|/2.$$

Then there exists a subgroup H of G with

$$|\mathcal{A} + H| < \min(|G|, |H| + |\mathcal{A}|)$$

such that $\mathcal{A}/H$ is either an arithmetic progression or a Vosper subset in G/H.

After having proved Theorem 2.1 in Section 3, we will apply it to (k, l)-free sets. We suspect that this result could be useful in several other contexts. For example, in [13], we obtain another application of this result to inverse additive number theory.

Our study of (k, l)-free sets will generalize all the results known in the case of sum-free sets. In the very case of sum-free sets, our approach leads to some improvement on the known results and give precisions on Yap's results.

In Section 4, using Theorem 2.1, we will first derive a structural result on "large" maximal (k, l)-free sets. To state this result, we let for any given finite set $\mathcal{X}$,

$$\epsilon(\mathcal{X}) = \begin{cases} 1 & \text{if } |\mathcal{X}| \text{ is odd,} \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 2.2. *Let k and l be two different positive integers. Let $\mathcal{A}$ be a maximal (k, l)-free set in an arbitrary finite Abelian group G. If*

$$(k + l)|\mathcal{A}| \geq |G| + 1 - \epsilon(G),$$

then there exists a subgroup H of G such that

- *$\mathcal{A} + H = \mathcal{A}$,*
- *G/H is a cyclic group,*
- *$\mathcal{A}/H$ is an arithmetic progression, and,*
- *$\mathcal{A}/H$ is a maximal (k, l)-free set.*

In Section 5, we investigate the value of $\lambda_{k,l}(G)$. We first derive a general result. As it will turn out from our approach, the natural parameter to be introduced is

$$\alpha_{k,l}(d)$$

the *maximal cardinality of a (k, l)-free arithmetic progression in a cyclic group of order d* (or, equivalently, in $\mathbb{Z}/d\mathbb{Z}$). In particular, any (k, l)-free arithmetic progression in $\mathbb{Z}/d\mathbb{Z}$ with cardinality $\alpha_{k,l}(d)$ is a maximal (k, l)-free arithmetic progression. With this notation, the main result of Section 5 is the following theorem.

Theorem 2.3. *Let k and l be two different positive integers. Let G be any finite Abelian group. Then*

$$\max_{d | \exp(G)} \frac{\alpha_{k,l}(d)|G|}{d} \leq \lambda_{k,l}(G) \leq \max\left(\frac{|G| - \epsilon(G)}{k + l}, \max_{d | \exp(G)} \frac{\alpha_{k,l}(d)|G|}{d}\right).$$

This theorem can be completely elucidated in the case where $\gcd(k-l, |G|) = 1$, an hypothesis which is automatically satisfied in the case of sum-free sets since $k - l = 1$. In the absence of this assumption, degenerate behaviors may appear:

for instance, if $k \equiv l \pmod{\exp(G)}$, then $\lambda_{k,l}(G) = 0$. From now on (except in Section 4), we always assume $\gcd(k-l, |G|) = 1$.

A consequence of Theorem 2.3 is the following explicit result.

Theorem 2.4. *Let k and l be two different positive integers. Let G be any finite Abelian group such that* $\gcd(|G|, k-l) = 1$. *If* $\exp(G)$ *possesses at least one divisor not congruent to* $1 \pmod{k+l}$ *then*

$$\lambda_{k,l}(G) = \max_{d \mid \exp(G)} \left\{ \frac{[(d-2)/(k+l)]+1}{d} \right\} |G|.$$

This corollary generalizes Theorem C. On the more, it follows from our study a more general understanding of the very nature of the obstruction in determining $\lambda_{2,1}(G)$ in case (iii) of Theorem C. Generally speaking, we are unable to compute $\lambda_{k,l}(G)$ in the case where any factor of the exponent of the group is congruent to 1 modulo $k+l$.

Nevertheless, Theorem 2.4 is a strong indication that the following Conjecture 2.5 (which generalizes Yap's Conjecture B in a reasonable way) could be true.

Conjecture 2.5. *Let k and l be two different positive integers. Let G be any finite Abelian group satisfying* $\gcd(|G|, k-l) = 1$, *then*

$$\lambda_{k,l}(G) = \max_{d \mid \exp(G)} \left\{ \frac{[(d-2)/(k+l)]+1}{d} \right\} |G|.$$

Actually, we can prove this conjecture in the case of cyclic groups.

Theorem 2.6. *Let k and l be two different positive integers, n be any positive integer such that* $\gcd(n, k-l) = 1$. *Then*

$$\lambda_{k,l}(\mathbb{Z}/n\mathbb{Z}) = \max_{d \mid n} \left\{ \frac{[(d-2)/(k+l)]+1}{d} \right\} n.$$

For n a prime, this result reduces to the evaluation of $\lambda_{k,l}(G)$ in Theorem D.

Finally, in Section 6, we apply the structural result derived in Section 4 (Theorem 2.2) to the case of sum-free sets. In Proposition 6.1, we will characterize completely, and for any finite Abelian group G, all the maximal sum-free sets in G with cardinality at least one third of that of G. This allows us not only to recover but also to extend the results quoted in the Introduction (both Theorem C and the structural characterization of sum-free sets with maximal cardinality (Theorems 7.8 and 7.9 in [28])).

3. A new addition theorem generalizing Vosper's

The most basic additive result in finite groups is the simple following lemma [18, Theorem 1.1]. It is an easy consequence of the pigeon-hole principle and sometimes referred to as the Prehistorical lemma.

Lemma 3.1 (Prehistorical lemma). *Let H be a finite subgroup of an arbitrary Abelian group G, $\mathcal{A}, \mathcal{B}$ be subsets of G, each being included in some H-coset. If $|\mathcal{A}| + |\mathcal{B}| > |H|$, then $|\mathcal{A} + \mathcal{B}| = |H|$.*

The following result slightly generalizes Theorem A and can be proved in a very similar way.

Lemma 3.2. *Let $\mathcal{A}$ be a generating subset of a finite Abelian group G such that $0 \in \mathcal{A}$ and $|\mathcal{A}| \leq (|G| + 1)/2$, then one of the following conditions holds:*
(i) *$\mathcal{A}$ is an arithmetic progression,*
(ii) *there is a subgroup $H \neq \{0\}$ such that $|H + \mathcal{A}| < \min(|G| - 1, |H| + |\mathcal{A}|)$,*
(iii) *$\mathcal{A}$ is a Vosper subset of G.*

Before proceeding with the proof and for the sake of clarity, it will be useful and efficient to introduce the needed vocabulary from the isoperimetric method (the reader interested in a general introduction to this subject is referred to [8, 9]). Doing so should make easier the forthcoming references to results from the isoperimetric method in the literature.

In order to save space, here is only what is needed to understand the following proof. Let G be an arbitrary finite Abelian group. In the context of the isoperimetric method, a subset $\mathcal{A}$ of G such that there exists a set $\mathcal{X}_0 \subset G$ with $|\mathcal{X}_0| \geq 2$ and $|\mathcal{A} + \mathcal{X}_0| \leq |G| - 2$ is said to be *2-separable.* In that case, the following minimum is well defined

$$\kappa_2(\mathcal{A}) = \min\{|\mathcal{A} + \mathcal{X}| - |\mathcal{X}| \text{ where } \mathcal{X} \subset G, |\mathcal{X}| \geq 2 \text{ and } |\mathcal{A} + \mathcal{X}| \leq |G| - 2\}$$

and known as the *second isoperimetric number.* Therefore, $\mathcal{A}$ is *not* a Vosper set if and only if it is 2-separable and verifies $\kappa_2(\mathcal{A}) \leq |\mathcal{A}| - 1$. A set $\mathcal{X}_1 \subset G$ such that $|\mathcal{X}_1| \geq 2$, $|\mathcal{A} + \mathcal{X}_1| \leq |G| - 2$ and $\kappa_2(\mathcal{A}) = |\mathcal{A} + \mathcal{X}_1| - |\mathcal{X}_1|$ is said to be *2-critical (for $\mathcal{A}$).* A 2-critical set with minimal cardinality is called a *2-atom (for $\mathcal{A}$).* Notice that the translate of a 2-atom (and more generally of a 2-critical set) is still a 2-atom (resp. a 2-critical set), so that we may always consider a 2-atom *containing* 0. The following result gives a structural characterization of the 2-atoms when the second isoperimetric number is "small".

Lemma 3.3. (Corollary 6.3 in [11]). *Let $\mathcal{A}$ be a subset of some finite Abelian group G such that $0 \in \mathcal{A}$. Let K be a 2-atom (for $\mathcal{A}$) containing 0.*
If $\kappa_2(\mathcal{A}) = |\mathcal{A}| - 1$, then either K is a subgroup of G or $|K| = 2$.
If $\kappa_2(\mathcal{A}) \leq |\mathcal{A}| - 2$, then K is a subgroup of G.

We will need yet another structural result on 2-atoms.

Lemma 3.4 (Proposition 6.5 in [11]). *Let $\mathcal{A}$ be a generating subset of some finite Abelian group G such that $0 \in \mathcal{A}$. We assume that $\kappa_2(\mathcal{A}) = |\mathcal{A}| - 1$, and let K be a 2-atom containing 0. Then, one of the following holds:*

- $|K| > 2$ *and K is a subgroup of G,*
- $\mathcal{A}$ *is an arithmetic progression,*
- $\mathcal{A}$ *is* almost periodic *: that is, $\mathcal{A}$ is the union of one element a and some J-cosets (not containing a) for some subgroup $J \neq \{0\}$ of G,*
- $|\mathcal{A}| > |G|/2$ *and there is a proper subgroup L of G such that $|\mathcal{A}| \geq |G| - |L| + 1$.*

Now, we are equipped enough to prove Lemma 3.2.

Proof of Lemma 3.2. In the case where $|\mathcal{A}| \leq |G|/2$, this is exactly Theorem A (or Lemma 2 of [12]). The only case which remains is that of groups G with odd cardinality and $|\mathcal{A}| = (|G| + 1)/2$.

If $\mathcal{A}$ is not a Vosper subset (that is, if (iii) is false), then, as noticed above, there is a set $\mathcal{X}_0$ with $|\mathcal{X}_0| \geq 2$ and $|\mathcal{A} + \mathcal{X}_0| \leq |G| - 2$; moreover

$$\kappa_2(\mathcal{A}) = \min\{|\mathcal{A} + \mathcal{X}| - |\mathcal{X}| \text{ where } \mathcal{X} \subset G, |\mathcal{X}| \geq 2 \text{ and } |\mathcal{A} + \mathcal{X}| \leq |G| - 2\}$$

verifies

$$\kappa_2(\mathcal{A}) \leq |\mathcal{A}| - 1.$$

Now, we consider K, a 2-atom containing 0.

If $\kappa_2(\mathcal{A}) \leq |\mathcal{A}| - 2$ or $|K| \geq 3$, then we can apply Lemma 3.3 which implies that K is a subgroup of G. Since K is a 2-atom, it contains at least two elements, so $K \neq \{0\}$. Thus we get (ii) with $H = K$.

From now on, we may therefore assume that $\kappa_2(\mathcal{A}) = |\mathcal{A}| - 1$ and $|K| = 2$. Thus, we are in a position to apply Lemma 3.4 from which it turns out that there are only three possible cases (the first case in the conclusion of Lemma 3.4 cannot happen).

In the first case ($\mathcal{A}$ is an arithmetic progression), we get directly (i).

In the second case ($\mathcal{A}$ is almost periodic), keeping the notation J for the subgroup introduced in Lemma 3.4, we obtain $|\mathcal{A} + J| = |\mathcal{A}| + |J| - 1$. Therefore $\mathcal{A} + J \neq G$, otherwise since $|\mathcal{A}| = (|G| + 1)/2$ we obtain $|J| = (|G| + 1)/2$, which is not possible. So,

$$|\mathcal{A} + J| \leq |G| - |J| \leq |G| - 2.$$

We are therefore in case (ii) with $H = J$ and the result follows.

The final case is the one where there is a proper subgroup L of G such that

$$|\mathcal{A}| \geq |G| - |L| + 1.$$

Since $|L| \leq |G|/3$ (G has an odd cardinality), we come to the contradiction

$$(|G| + 1)/2 = |\mathcal{A}| \geq |G| - |L| + 1 \geq 2|G|/3 + 1 > 2(|G| + 1)/3.$$

This achieves the proof. □

In order to prove Theorem 2.1, we will need yet another lemma.

Lemma 3.5. *Let G be any finite Abelian group and H be a subgroup of G. Let us put $\psi = \psi_{G,G/H}$. Let $\mathcal{A}$ be a subset of G such that*

$$|\mathcal{A} + H| < \min(|G|, |H| + |\mathcal{A}|).$$

If K is a subgroup of G/H such that

$$|\psi(\mathcal{A}) + K| < \min(|G|/|H|, |K| + |\psi(\mathcal{A})|),$$

then

$$|\mathcal{A} + \psi^{-1}(K)| < \min(|G|, |\mathcal{A}| + |\psi^{-1}(K)|).$$

Proof. Let us set $K' = \psi^{-1}(K)$ so that $K' + H = K'$. Thus $K' + \mathcal{A}$ is composed with H-cosets. Consequently, we obtain

$$\begin{aligned} |K' + \mathcal{A}| &= |H||\psi(K' + \mathcal{A})| \\ &= |H||K + \psi(\mathcal{A})| \\ &\leq |H|(|K| + |\psi(\mathcal{A})| - 1) \\ &= |H||K| + |\mathcal{A} + H| - |H| \\ &< |K'| + |\mathcal{A}|. \end{aligned}$$

Since $|K + \psi(\mathcal{A})| < |G/H|$, $K + \psi(\mathcal{A}) \neq G/H$ and thus $K' + \mathcal{A} \neq G$. The conclusion follows. □

We are now ready to prove our generalization of Vosper's theorem.

Proof of Theorem 2.1. Take H a maximal subgroup of G such that

$$|\mathcal{A} + H| < \min(|G|, |H| + |\mathcal{A}|).$$

Since $\{0\}$ satisfies this inequality, such a subgroup does exist.

Let us prove that

$$|\psi(\mathcal{A})| \leq \frac{|G/H| + 1}{2}, \tag{2}$$

where ψ denotes once again $\psi_{G,G/H}$. Indeed,

$$|\psi(\mathcal{A})||H| = |\mathcal{A} + H| < |H| + |\mathcal{A}|$$

and thus

$$|\psi(\mathcal{A})| < \frac{|\mathcal{A}|}{|H|} + 1 \leq \frac{|G|/2}{|H|} + 1 = \frac{|G/H|}{2} + 1,$$

which gives (2).

Clearly $0 \in \psi(\mathcal{A})$ and $\psi(\mathcal{A})$ is a generating set in G/H. We are thus in a position to apply Lemma 3.2 to $\mathcal{A}/H$ and G/H. The result follows since case (ii) cannot happen. Indeed, for any non-zero subgroup K of G/H,

$$|K+\psi(\mathcal{A})| \geq \min(|G/H|, |K|+|\psi(\mathcal{A})|),$$

in view of the maximality of H (the set $\psi^{-1}(K)$ contains H) and Lemma 3.5. □

4. A structural result on "large" maximal (k,l)-free sets

Let us begin with two easy remarks that we state under the form of a lemma. It will be useful in what follows.

Lemma 4.1. *Let k and l be two different positive integers. Let G be an Abelian group and H be a subgroup of G. If $\mathcal{X}$ is a (k,l)-free set in G/H, then the inverse image of $\mathcal{X}$, $\psi^{-1}_{G,G/H}(\mathcal{X})$, is a (k,l)-free set in G. Moreover, if $\psi^{-1}_{G,G/H}(\mathcal{X})$ is a maximal (k,l)-free set in G, then $\mathcal{X}$ is a maximal (k,l)-free set in G/H.*

We shall also need the following two lemmas (we have included a short proof of Lemma 4.2 in [12]).

Lemma 4.2 (Olson's lemma [20]) *Let $\mathcal{B}$ be a generating subset of a finite Abelian group G such that $0 \in \mathcal{B}$. Then for every non-empty subset $\mathcal{C}$ of G, we have*

$$|\mathcal{B}+\mathcal{C}| \geq \min(|G|, |\mathcal{B}|/2+|\mathcal{C}|).$$

In particular, for every positive integer j, we have

$$|j\mathcal{B}| \geq \min\left(|G|, \left\lceil \frac{(j-1)|\mathcal{B}|}{2} \right\rceil + |\mathcal{B}|\right).$$

Lemma 4.3. *Let k and l be two different positive integers. Let G be a finite Abelian group which admits a maximal (k,l)-free set with one element. Then G is a cyclic group.*

Proof. We assume the existence of a maximal (k,l)-free set with one element, say $\{\alpha\}$. It is well known that any finite Abelian group is isomorphic to some

$$\mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \cdots \times \mathbb{Z}/a_{s-1}\mathbb{Z} \times \mathbb{Z}/a_s\mathbb{Z}$$

with $2 \leq a_s | a_{s-1} | \dots | a_2 | a_1$ (see for example [23]). So, we may assume that G is of this form. Suppose that $s \geq 2$ and write α in $\mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \cdots \times \mathbb{Z}/a_s\mathbb{Z}$ as

$$\alpha = (\alpha_1, \alpha_2, \dots, \alpha_s).$$

Since the set $\{\alpha\}$ is a maximal (k,l)-free set, we have $0 \in k\{\alpha,\beta\} - l\{\alpha,\beta\}$ for any $\beta \in G$, different from α. Apply this for instance to $\beta = (\alpha_1, \alpha_2+1, \alpha_3, \dots, \alpha_s)$.

Since any element of $k\{\alpha,\beta\} - l\{\alpha,\beta\}$ has $(k-l)\alpha_1$ as its first coordinate we deduce that

$$(k-l)\alpha_1 = 0.$$

Clearly, there was nothing specific with the first coordinate in this reasoning so that we infer more generally that $(k-l)\alpha_i = 0$ for any i $(1 \leq i \leq s)$. This shows that $k\alpha = l\alpha$, or, in other words that $\{\alpha\}$ is not (k,l)-free. This is a contradiction; thus $s = 1$ and G is cyclic. $\square$

We are now ready to prove our main result of this section, namely Theorem 2.2.

Proof of Theorem 2.2. In this proof we assume without loss of generality that $k > l$.

In the first part of the proof, we consider only the case where there is an $a \in \mathcal{A}$ such that $\mathcal{A} - a$ generates G. Let us fix such an element a and write $\mathcal{B} = \mathcal{A} - a$.

By Theorem 2.1 (0 belongs to $\mathcal{B}$ and $|\mathcal{B}| = |\mathcal{A}| \leq |G|/2$ by (1)), there exists a subgroup H of G with

$$|\mathcal{B} + H| < \min(|G|, |H| + |\mathcal{B}|) \tag{3}$$

and such that $\mathcal{B}/H$ is either an arithmetic progression or a Vosper subset in G/H.

We now define a partition of $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_u$, with $|\mathcal{B}_1| \leq \cdots \leq |\mathcal{B}_u|$ such that any $\mathcal{B}_i$ is the intersection of $\mathcal{B}$ with an H-coset. Note that $u \geq 2$ follows from the fact that $\mathcal{B}$ generates G.

By (3), we get

$$(u-1)|H| < |\mathcal{B}_1| + \cdots + |\mathcal{B}_u|.$$

Since each $\mathcal{B}_i$ has cardinality at most $|H|$, it follows that for any $(i,j) \neq (1,1)$,

$$|\mathcal{B}_i| + |\mathcal{B}_j| \geq |H| + 1. \tag{4}$$

By Lemma 3.1, we get $\mathcal{B}_i + \mathcal{B}_j = \mathcal{B}_i + \mathcal{B}_j + H$. It follows that if $r \geq 2$,

$$r\mathcal{B} = \big(r(\mathcal{B}+H) \setminus (r\mathcal{B}_1 + H)\big) \cup r\mathcal{B}_1, \tag{5}$$

and also, for any $r, t \geq 1$,

$$r\mathcal{B} - t\mathcal{B} = \big(r(\mathcal{B}+H) - t(\mathcal{B}+H) \setminus (r\mathcal{B}_1 - t\mathcal{B}_1 + H)\big) \cup (r\mathcal{B}_1 - t\mathcal{B}_1). \tag{6}$$

Now, we claim that $\mathcal{B}/H$ is an arithmetic progression in G/H. Indeed, let us assume the contrary. In particular, we have

$$u = |\mathcal{B}/H| \geq 3$$

and $\mathcal{B}/H$ has to be a Vosper subset of G/H.

Let us prove that the following inequality holds:

$$|(k-l)\mathcal{B}| \geq (k-l)|\mathcal{B}|. \tag{7}$$

Since it is clearly valid when $k - l = 1$, we may assume that $k - l \geq 2$. The (k,l)-freeness of $\mathcal{A}$ implies that $(k-l)\mathcal{A}$ and $l\mathcal{A} - l\mathcal{A}$ are intersection-free. By using this, (5) and (4), we obtain

$$\begin{aligned}
|G| &\geq |(k-l)\mathcal{A}| + |l\mathcal{A} - l\mathcal{A}| \\
&= |(k-l)\mathcal{B}| + |l\mathcal{B} - l\mathcal{B}| \\
&\geq |(k-l)\mathcal{B}| + |\mathcal{B}| \\
&\geq (|(k-l)(\mathcal{B}+H)| - |(k-l)\mathcal{B}_1 + H| + |(k-l)\mathcal{B}_1|) + (|\mathcal{B}_1| + |\mathcal{B}_2| + |\mathcal{B}_3|) \\
&\geq (|(k-l)(\mathcal{B}+H)| - |H| + |\mathcal{B}_1|) + (|\mathcal{B}_1| + |\mathcal{B}_2| + |\mathcal{B}_3|) \\
&= |(k-l)(\mathcal{B}+H)| - |H| + (|\mathcal{B}_1| + |\mathcal{B}_2|) + (|\mathcal{B}_1| + |\mathcal{B}_3|) \\
&> |(k-l)(\mathcal{B}+H)| + |H|.
\end{aligned}$$

Therefore $|(k-l)(\mathcal{B}+H)|$ which is a multiple of $|H|$ verifies

$$|(k-l)(\mathcal{B}+H)| \leq |G| - 2|H|$$

or equivalently (notice that for any subset $\mathcal{C}$ of G, we have $(\mathcal{C}+H)/H = \mathcal{C}/H$)

$$|(k-l)\mathcal{B}/H| \leq |G/H| - 2.$$

Thus, by a repeated application of the Vosper subset property, we obtain that

$$|(k-l)\mathcal{B}/H| \geq (k-l)|\mathcal{B}/H|$$

or

$$|(k-l)(\mathcal{B}+H)| \geq (k-l)|\mathcal{B}+H|.$$

We thus deduce (by (5) and this)

$$\begin{aligned}
|(k-l)\mathcal{B}| &\geq |(k-l)(\mathcal{B}+H)| - |(k-l)\mathcal{B}_1 + H| + |(k-l)\mathcal{B}_1| \\
&\geq (k-l)|\mathcal{B}+H| - |H| + |\mathcal{B}_1| \\
&\geq (k-l)|\mathcal{B}|,
\end{aligned}$$

and (7) is proved.

In the same way, we also have (by (6) and the Vosper subset property for $\mathcal{B}+H$) that

$$\begin{aligned}
|l\mathcal{B} - l\mathcal{B}| &\geq |l(\mathcal{B}+H) - l(\mathcal{B}+H)| - |(l\mathcal{B}_1 - l\mathcal{B}_1) + H| + |l\mathcal{B}_1 - l\mathcal{B}_1| \\
&\geq 2l|\mathcal{B}+H| - |H| + |\mathcal{B}_1| \\
&\geq 2l|\mathcal{B}|.
\end{aligned}$$

Now, $l\mathcal{B} - l\mathcal{B}$ is *symmetric around zero* by which we mean that if x belongs to it then so does $-x$. Therefore, if G has an odd cardinality and since $\mathcal{B}$ contains 0, the cardinality of $l\mathcal{B} - l\mathcal{B}$ must be odd. We thus have

$$|l\mathcal{B} - l\mathcal{B}| \geq 2l|\mathcal{B}| + \epsilon(G). \tag{8}$$

By using (7) and (8), we finally obtain

$$\begin{aligned}
|G| &\geq |l\mathcal{B} - l\mathcal{B}| + |(k-l)\mathcal{B}| \\
&\geq (k+l)|\mathcal{B}| + \epsilon(G),
\end{aligned}$$

in contradiction with the hypothesis on $|\mathcal{B}| = |\mathcal{A}|$. Thus $\mathcal{B}/H$ is an arithmetic progression. So does $\mathcal{A}/H$, which is one of its translates.

We immediately note that G/H is cyclic. Indeed, $\mathcal{B}/H$ is at the same time a generating subset and an arithmetic progression containing 0.

We now claim that $\mathcal{A}/H$ itself is (k,l)-free. Indeed, assume the contrary and define

$$\mathcal{A}_i = \mathcal{B}_i + a.$$

Then, by a translation of (6) (with $r = k, t = l$),

$$0 \in k\mathcal{A}_1 - l\mathcal{A}_1 + H.$$

Since $\mathcal{A}_1$ is contained in exactly one H-coset, we deduce that

$$k\mathcal{A}_1 - l\mathcal{A}_1 + H = H.$$

This implies

$$(k-l)\mathcal{A}_1 \subset k\mathcal{A}_1 - l\mathcal{A}_1 \subset k\mathcal{A}_1 - l\mathcal{A}_1 + H = H.$$

Thus, $l\mathcal{A}_2$ and $(k-l)\mathcal{A}_1 + l\mathcal{A}_2$ are contained in the same H-coset. In fact, the latter set is a whole H-coset (by (4) and Lemma 3.1). Therefore

$$l\mathcal{A}_2 \subset (k-l)\mathcal{A}_1 + l\mathcal{A}_2 \subset k\mathcal{A}.$$

On the other hand, $l\mathcal{A}_2 \subset l\mathcal{A}$. Thus $k\mathcal{A} \cap l\mathcal{A} \supset l\mathcal{A}_2 \neq \emptyset$, which contradicts the assumption $k\mathcal{A} \cap l\mathcal{A} = \emptyset$. We have therefore proved that $\mathcal{A}/H$ is a (k,l)-free set.

Now, by Lemma 4.1, $\mathcal{A} + H = \psi^{-1}_{G,G/H}(\mathcal{A}/H)$ is (k,l)-free. The maximality of $\mathcal{A}$ then implies $\mathcal{A} = \mathcal{A} + H$. So, $\mathcal{A} = \psi^{-1}_{G,G/H}(\mathcal{A}/H)$ being maximal, Lemma 4.1 again shows that $\mathcal{A}/H$ itself has to be a maximal (k,l)-free set in G/H. This closes the first part of this proof.

We now come to the second possible case, namely the case where there is no element $a \in \mathcal{A}$ such that $\mathcal{B} = \mathcal{A} - a$ generates G. We select an arbitrary element $a \in \mathcal{A}$. The set $\mathcal{B} = \mathcal{A} - a$ generates a *proper* subgroup, say K, of G. We have $\mathcal{A} \subset a + K$ and $\mathcal{B} \subset K$.

Assume that $(k-l)a$ belongs to K. So, $k\mathcal{A}$ and $l\mathcal{A}$ are two disjoint (by (k,l)-freeness) subsets of the same K-coset. We thus get

$$|k\mathcal{B}| + |l\mathcal{B}| = |k\mathcal{A}| + |l\mathcal{A}| \leq |K| \leq |G|/2. \tag{9}$$

Since $\mathcal{B}$ generates K and contains 0, we are in a position to apply Lemma 4.2 (notice that $|k\mathcal{B}|, |l\mathcal{B}| < |K|$) which gives

$$|k\mathcal{B}| + |l\mathcal{B}| \geq \left(\left\lceil \frac{(k-1)|\mathcal{B}|}{2} \right\rceil + |\mathcal{B}| \right) + \left(\left\lceil \frac{(l-1)|\mathcal{B}|}{2} \right\rceil + |\mathcal{B}| \right) \geq \frac{k+l+2}{2}|\mathcal{B}|.$$

This and (9) give

$$|\mathcal{A}| = |\mathcal{B}| \leq \frac{|G|}{k+l+2},$$

in contradiction with the assumption on the cardinality of $\mathcal{A}$ in the statement of Theorem 2.2. Consequently, $(k-l)a$ does not belong to K.

Since ka and la do not fall in the same K-coset, the set $a+K$ itself is (k,l)-free. Therefore, the maximality of $\mathcal{A}$ implies that $\mathcal{A}=a+K$. Thus $\mathcal{A}+K=\mathcal{A}$. Since $\mathcal{A}=\psi_{G,G/K}^{-1}(\mathcal{A}/K)$ is a maximal (k,l)-free set, Lemma 4.1 shows that $\mathcal{A}/K$ itself is a maximal (k,l)-free set in G/K. Finally, the cyclicity of G/K follows from Lemma 4.3 and the second possible case is now completed. □

5. Large (k,l)-free sets

5.1. Proof of Theorem 2.3

Let us first recall the following lemma which is an easy exercise.

Lemma 5.1. *Let G be any finite Abelian group. For any integer m, the two following propositions are equivalent:*

(i) *m divides $\exp G$,*

(ii) *there exists a subgroup H of G such that G/H is isomorphic to $\mathbb{Z}/m\mathbb{Z}$.*

We go on with another lemma.

Lemma 5.2. *Let k and l be two different positive integers. Let G be a finite Abelian group and m any divisor of $\exp(G)$. Then there exists a (k,l)-free set in G with cardinality*

$$\frac{\alpha_{k,l}(m)}{m}|G|.$$

Proof. Since m divides the exponent of G, by Lemma 5.1, there exists a subgroup H of G, such that G/H is isomorphic to $\mathbb{Z}/m\mathbb{Z}$. Choose a (k,l)-free set $\mathcal{A}$ in arithmetic progression in $\mathbb{Z}/m\mathbb{Z}$ with cardinality $\alpha_{k,l}(m)$. Finally, consider the inverse image of it $P=\psi_{G,G/H}^{-1}(\mathcal{A})$. The set P has cardinality $\alpha_{k,l}(m)|H| = \alpha_{k,l}(m)|G|/m$ and is (k,l)-free by Lemma 4.1. □

An immediate consequence of Lemma 5.2 is the proof of the lower bound

$$\lambda_{k,l}(G) \geq \max_{d|\exp(G)} \frac{\alpha_{k,l}(d)}{d}|G|. \tag{10}$$

Let us now come to the upper bound.

Consider $\mathcal{A}$ a (k,l)-free subset of G with maximal cardinality (and consequently maximal itself), and assume

$$(k+l)|\mathcal{A}| \geq |G|+1-\epsilon(G). \tag{11}$$

We can apply Theorem 2.2 by which we know that there is a subgroup H of G such that $\mathcal{A}+H=\mathcal{A}$, $\mathcal{A}/H$ is both a maximal (k,l)-free set in G/H and an arithmetic progression and, finally, G/H is cyclic. We shall write $m=|G/H|$. By Lemma 5.1, the cyclicity of G/H implies $m|\exp(G)$.

Since $|\mathcal{A}|$ has maximal cardinality and $\mathcal{A}=\mathcal{A}+H$, it follows from Lemma 4.1 that $|\mathcal{A}/H|=|\mathcal{A}|/|H|$ is the maximal possible cardinality of a (k,l)-free arithmetic progression in the cyclic group of order $|G/H|$, that is exactly $\alpha_{k,l}(m)$. Thus

$$|\mathcal{A}|=\alpha_{k,l}(m)|H|=\alpha_{k,l}(m)\frac{|G|}{m}.$$

This achieves the proof of Theorem 2.3.

5.2. Preparatory lemmas

In this section, we study the function $\alpha_{k,l}(n)$ defined as the maximal cardinality of a (k,l)-free arithmetic progression in $\mathbb{Z}/n\mathbb{Z}$. Clearly $\alpha_{k,l}(1)=0$ so that we shall assume $n\geq 2$. Our goal is the proof of the following lemma.

Lemma 5.3. *Let $n\geq 2$, k and l be three positive integers subject to $k\neq l$ and*

$$\gcd(n,k-l)=1.$$

Then $\alpha_{k,l}(n)$ is given by the formula

$$\alpha_{k,l}(n)=\max\left(\frac{n}{p},\left[\frac{n-2}{k+l}\right]+1\right),$$

where p denotes the smallest prime dividing n.

It turns out that the proof of Lemma 5.3 must be divided according to whether or not the arithmetic progression considered is contained in a coset of a proper subgroup (in short, we shall call such a coset, a *proper* coset). That is why we define two new quantities. For $n\geq 2$, we let

$$\beta_{k,l}(n)$$

denote the *maximal cardinality of a (k,l)-free arithmetic progression in $\mathbb{Z}/n\mathbb{Z}$ contained in some proper coset* and let

$$\gamma_{k,l}(n)$$

denote the *maximal cardinality of (k,l)-free arithmetic progression in $\mathbb{Z}/n\mathbb{Z}$ not contained in any proper coset* (if there is no such (k,l)-free arithmetic progression in $\mathbb{Z}/n\mathbb{Z}$, then we put $\gamma_{k,l}(n)=0$).

Clearly $\alpha_{k,l}(n)=\max(\beta_{k,l}(n),\gamma_{k,l}(n))$. Thus, Lemma 5.3 is an easy consequence of the two following lemmas (Lemmas 5.4 and 5.5).

Lemma 5.4. *Let $n \geq 2$, k and l be three positive integers subject to $k \neq l$ and*

$$\gcd(n, k-l) = 1,$$

then $\beta_{k,l}(n)$ is equal to n/p where p denotes the smallest prime dividing n.

Proof. Let P be a (k,l)-free arithmetic progression, contained in some proper coset in $\mathbb{Z}/n\mathbb{Z}$, with the maximal possible cardinality for the sets with these properties. By definition, P is included in a certain coset of the form $a + H$ for some proper subgroup H of G. Therefore, the size of P is less than or equal to the maximal size of any proper subgroup of $\mathbb{Z}/n\mathbb{Z}$, that is $|P| \leq n/p$. Therefore $\beta_{k,l}(n) \leq n/p$.

Conversely, given any subgroup H of $\mathbb{Z}/n\mathbb{Z}$, if we choose a in $\mathbb{Z}/n\mathbb{Z}$ such that $(k-l)a \notin H$ (which is always possible by the coprimality condition), the H-coset $a+H$ is an arithmetic progression (since H is cyclic) which is (k,l)-free, contained in a proper coset and has cardinality $|H|$. Taking for H the subgroup of multiples of p gives $\beta_{k,l}(n) \geq n/p$. □

Having in mind the forthcoming Lemma 5.7, we underline the fact that there *are* (k,l)-free arithmetic progressions contained in some proper coset with cardinality $\beta_{k,l}(n)$ in $\mathbb{Z}/n\mathbb{Z}$ which are *not* maximal (k,l)-free sets. For instance, we may consider the set $\{2,7,12,17,22\} \subset \mathbb{Z}/25\mathbb{Z}$ which is not a maximal sum-free set since it is a subset of $\{2,3,7,12,17,22\}$ (which *is still* sum-free). We shall see that the situation is completely different for (k,l)-free arithmetic progressions *not* contained in a proper coset with maximal cardinality $\gamma_{k,l}(n)$, that we start to study in the next lemma.

Lemma 5.5. *Let $n \geq 2$, k and l be three positive integers subject to $k \neq l$ and*

$$\gcd(n, k-l) = 1,$$

then $\gamma_{k,l}(n)$ is equal to

$$\gamma_{k,l}(n) = \begin{cases} \left\lfloor \frac{n-2}{k+l} \right\rfloor + 1, & \text{if } n \geq k+l+2, \\ 0, & \text{if } n \leq k+l+1. \end{cases}$$

Proof. We first show that, in $\mathbb{Z}/n\mathbb{Z}$, the cardinality of any (k,l)-free arithmetic progression not contained in any proper coset is upper bounded by

$$\left\lfloor \frac{n-2}{k+l} \right\rfloor + 1. \tag{12}$$

To prove it, just consider any arithmetic progression P, not contained in a proper coset. The set P is of the form $P = \{x + jd, j = 0, 1, \ldots, j_0\}$ with d a non-zero element of $\mathbb{Z}/n\mathbb{Z}$ and j_0 some non-negative integer. By hypothesis, d generates $\mathbb{Z}/n\mathbb{Z}$ ($P - x$ is contained in the subgroup generated by d). Since P is an arithmetic progression, $kP - lP$ is also an arithmetic progression. It has

$$|kP - lP| = (k+l)(|P|-1) + 1 \tag{13}$$

elements. Indeed, $kP - lP = \{(k-l)x + jd, j = -lj_0, \ldots, kj_0\}$ and, by definition of (k,l)-freeness, 0 is not in $kP - lP$, therefore no element of $\mathbb{Z}/n\mathbb{Z}$ appears twice in the list $(k-l)x + jd$, $(j = -lj_0, \ldots, kj_0)$: would it be so, d being a generating element, jd would describe a complete set of residues modulo n and 0 would belong to $kP - lP$. This proves formula (13). Using again the (k,l)-freeness yields

$$(k+l)(|P|-1)+1 = |kP - lP| \leq n-1,$$

which gives the upper bound (12) for $|P|$.

If $n \leq k+l+1$, the upper bound (12) gives $\gamma_{k,l}(n) \leq 1$. But since any set with one element is included in a proper coset, we conclude that there is no (k,l)-free arithmetic progression not contained in a proper coset in $\mathbb{Z}/n\mathbb{Z}$ and that $\gamma_{k,l}(n) = 0$.

Suppose now $n \geq k+l+2$. In order to prove that $\gamma_{k,l}(n) = [(n-2)/(k+l)]+1$, we just need to construct a (k,l)-free arithmetic progression in $\mathbb{Z}/n\mathbb{Z}$, not contained in any proper coset, with that number of elements. Let us perform the Euclidean division $n-2 = (k+l)q + r$, $0 \leq r \leq k+l-1$ and notice that $q \geq 1$. Let us consider the arithmetic progression $P = \{x, x+1, \ldots, x+q\}$ with x the solution of $(k-l)x \equiv 1 + lq \pmod{n}$ which is possible by the coprimality condition. Clearly P, which contains $q+1 \geq 2$ consecutive elements cannot be included in a proper coset. Now,

$$kP - lP = \{(k-l)x + j, j = -lq, \ldots, kq\} = \{1, 2, \ldots, 1 + (k+l)q\}$$

which shows that P is a solution $(0 \notin kP - lP)$ since $1 + (k+l)q = n - 1 - r < n$. $\square$

Notice that, with this proof, it is easily seen what exactly the sets attaining the bound $\gamma_{k,l}(n)$ are. For a set $\mathcal{A} \subset G$ and j a positive integer, we shall denote by $j.\mathcal{A}$ the j-fold multiple set

$$j.\mathcal{A} = \{ja \text{ where } a \in \mathcal{A}\}.$$

Lemma 5.6. *Let n, k and l be three positive integers subject to $n \geq k+l+2$ and $k \neq l$ and*

$$\gcd(n, k-l) = 1.$$

The (k,l)-free arithmetic progressions, not contained in any proper coset, with cardinality $\gamma_{k,l}(n)$ in $\mathbb{Z}/n\mathbb{Z}$ are exactly the sets

$$d.\{x + j : j = 0, 1, \ldots, [(n-2)/(k+l)]\} \pmod{n}$$

where $d, x \in \mathbb{Z}/n\mathbb{Z}$, with d invertible and

$$(k-l)x \in \left\{ \left[\frac{n-2}{k+l}\right] l + 1, \ldots, n - \left[\frac{n-2}{k+l}\right] k - 1 \right\}.$$

For given n, k and l satisfying the assumptions of the lemma, the set of arithmetic progressions listed in Lemma 5.6 (which is never empty) will be denoted by

$\mathcal{GP}_{k,l}(\mathbb{Z}/n\mathbb{Z})$. By isomorphism, we can extend this notation to any cyclic group. So, for any cyclic group G such that $\gcd(|G|, k-l) = 1$ and $|G| \geq k+l+2$, we denote by

$$\mathcal{GP}_{k,l}(G)$$

the set of (k,l)-free arithmetic progressions, not contained in any proper coset, with cardinality $\gamma_{k,l}(|G|)$. This notation will be useful to describe the large maximal sum-free sets (this will be done in Section 6). The elements of these sets (or equivalently the elements of $\mathcal{GP}_{k,l}(\mathbb{Z}/n\mathbb{Z})$) have an interesting property for our purpose which contrasts with the situation described after Lemma 5.4: they are not only maximal (k,l)-free arithmetic progressions but also maximal (k,l)-free sets.

Lemma 5.7. *Let n, k and l be three positive integers subject to $n \geq k+l+2$ and*

$$\gcd(n, k-l) = 1.$$

Any element of $\mathcal{GP}_{k,l}(\mathbb{Z}/n\mathbb{Z})$ is a maximal (k,l)-free set.

Proof. We begin with a remark. If $\mathcal{C}$ is a non-empty subset of $\mathbb{Z}/n\mathbb{Z}$, we denote by $\mu_{\mathcal{C}}$ the smallest integer m such that $\mathcal{C}$ can be written as a union of m arithmetic progressions with difference 1. We clearly have, for any non-empty $\mathcal{C} \subset \mathbb{Z}/n\mathbb{Z}$,

$$|\mathcal{C} + \{0,1\}| \geq \min(|\mathcal{C}| + \mu_{\mathcal{C}}, n) \geq \min(|\mathcal{C}| + 1, n). \tag{14}$$

If R is an arithmetic progression with difference 1 (and $|R| \geq 2$), it is a translate of $(|R|-1)\{0,1\}$ which gives, using iteratively (14),

$$|\mathcal{C} + R| = |\mathcal{C} + (|R|-1)\{0,1\}| \geq \min(|\mathcal{C}| + |R| - 1, n). \tag{15}$$

If $\mathcal{C}$ is not an arithmetic progression with difference 1 and is non-empty, we have $\mu_{\mathcal{C}} \geq 2$ and (15) can be improved in

$$|\mathcal{C} + R| \geq \min(|\mathcal{C}| + |R|, n). \tag{16}$$

This follows, by (15) and (14), in view of

$$\begin{aligned} |\mathcal{C} + R| = |\mathcal{C} + \{0,1\} + (|R|-2)\{0,1\}| &\geq \min(|\mathcal{C} + \{0,1\}| + |R| - 2, n) \\ &\geq \min(|\mathcal{C}| + \mu_{\mathcal{C}} + |R| - 2, n). \end{aligned}$$

Now, take any arithmetic progression P in $\mathcal{GP}_{k,l}(\mathbb{Z}/n\mathbb{Z})$. Without loss of generality, we may assume that its difference is 1. Let $\mathcal{Q}$ be a subset of $\mathbb{Z}/n\mathbb{Z}$, containing P, such that $|\mathcal{Q}| = |P| + 1$. We assume that it is a (k,l)-free set. By definition of $P \in \mathcal{GP}_{k,l}(\mathbb{Z}/n\mathbb{Z})$, $\mathcal{Q}$ cannot be an arithmetic progression. So we have $\mu_{\mathcal{Q}} \geq 2$.

We now prove by induction that for any j subsets $\mathcal{Q}_1, \dots, \mathcal{Q}_j$ of $\mathbb{Z}/n\mathbb{Z}$ all equal to either $\mathcal{Q}$ or $-\mathcal{Q}$, we have

$$|\mathcal{Q}_1 + \cdots + \mathcal{Q}_j| \geq \min(1 + j|P|, n). \tag{17}$$

For $j = 1$, $|\mathcal{Q}_1| = |P| + 1$ and the formula holds. Let now j be a positive integer and assume that (17) holds for j. Without loss of generality, we may assume

$\mathcal{Q}_{j+1} = \mathcal{Q}$. We distinguish two cases. If $\mathcal{Q}_1 + \cdots + \mathcal{Q}_j$ is *not* an arithmetic progression with difference 1, we get by (16),

$$|\mathcal{Q}_1 + \cdots + \mathcal{Q}_j + \mathcal{Q}| \geq |\mathcal{Q}_1 + \cdots + \mathcal{Q}_j + P| \geq \min(|\mathcal{Q}_1 + \cdots + \mathcal{Q}_j| + |P|, n)$$

and the result holds in view of the induction hypothesis. If $\mathcal{Q}_1 + \cdots + \mathcal{Q}_j$ *is* an arithmetic progression with difference 1, we get by (15),

$$|\mathcal{Q}_1 + \cdots + \mathcal{Q}_j + \mathcal{Q}| \geq \min(|\mathcal{Q}_1 + \cdots + \mathcal{Q}_j| + |\mathcal{Q}| - 1, n) \geq \min(1 + j|P| + |P|, n),$$

and the result holds also. Thus, assertion (17) is proved.

Now, using this formula, we obtain

$$|k\mathcal{Q} - l\mathcal{Q}| \geq \min(1 + (k+l)|P|, n) = \min\left(1 + (k+l)\gamma_{k,l}(n), n\right) \geq n,$$

in contradiction with the (k,l)-freeness of $\mathcal{Q}$. □

5.3. Proof of Theorem 2.4

Again, we begin with a lemma.

Lemma 5.8. *Let k and l be two different positive integers and G be any finite Abelian group such that* $\gcd(|G|, k-l) = 1$. *Then*

$$\max_{d|\exp(G)} \frac{\alpha_{k,l}(d)}{d} = \max_{d|\exp(G)} \frac{[(d-2)/(k+l)] + 1}{d}.$$

Proof. When $d = 1$, the quantity $([(d-2)/(k+l)] + 1)/d = 0$. Thus the formula holds when $|G| = 1$. Assume now $|G| \geq 2$. By Lemma 5.3, we obtain, for any d dividing $\exp G$ ($d \geq 2$),

$$\alpha_{k,l}(d) = \max\left(\frac{d}{p_d}, \left[\frac{d-2}{k+l}\right] + 1\right),$$

where p_d denotes the smallest prime dividing d.

Since $\alpha_{k,l}(d)$ is a non-negative function vanishing in $d = 0$, we get

$$\max_{d|\exp(G)} \frac{\alpha_{k,l}(d)}{d} = \max_{d|\exp(G),\ d\geq 2} \frac{\alpha_{k,l}(d)}{d} = \max_{d|\exp(G),\ d\geq 2} \left(\max\left(\frac{d}{p_d}, \left[\frac{d-2}{k+l}\right] + 1\right)\right)\frac{1}{d}$$
$$= \max\left(\frac{1}{p}, \max_{d|\exp(G)}\left(\frac{[(d-2)/(k+l)]+1}{d}\right)\right)$$

where p is the smallest prime dividing $|G|$. But, since p divides the exponent of G and

$$\frac{[(p-2)/(k+l)] + 1}{p} \geq \frac{1}{p},$$

the preceding expression simplifies as announced. □

Let us now turn our attention to proving Theorem 2.4.

Proof of Theorem 2.4. Suppose first that the cardinality of G is even. Then, the coprimality hypothesis implies that $k-l$ is odd. Therefore, by considering any subgroup H of G with index 2 and the sum-free set $\mathcal{A} = G \setminus H$, we see that $\lambda_{k,l}(G) \geq |G|/2$. By (1), this gives $\lambda_{k,l}(G) = |G|/2$. On the other hand, we have

$$\frac{[(d-2)/(k+l)]+1}{d} \quad \begin{cases} = 1/2 \text{ if } d = 2 \\ < 1/2 \text{ if } d \geq 3. \end{cases}$$

This gives the result.

Now, we consider the case of groups with an odd cardinality (that is, the case $\epsilon(G) = 1$). Applying Lemma 5.8 to the lower bound in Theorem 2.3 yields

$$\lambda_{k,l}(G) \geq \max_{d|\exp(G)} \left(\frac{[(d-2)/(k+l)]+1}{d} \right) |G|, \tag{18}$$

which is half of the formula of Theorem 2.4.

Since, by hypothesis, $\exp(G)$ has a divisor m which is not congruent to 1 modulo $k+l$, we may find an integer r with $2 \leq r \leq k+l$ and $m \equiv r \pmod{k+l}$. Then

$$\left[\frac{m-2}{k+l}\right] + 1 = \frac{(m-r+k+l)}{k+l} \geq \frac{m}{k+l}. \tag{19}$$

This shows, using (18), that

$$\lambda_{k,l}(G) \geq \frac{|G|}{k+l}.$$

Therefore, once again by Theorem 2.3 (but using now the upper bound), we get

$$\lambda_{k,l}(G) \leq \max_{d|\exp(G)} \frac{\alpha_{k,l}(d)|G|}{d} = \max_{d|\exp(G)} \left(\frac{[(d-2)/(k+l)]+1}{d} \right) |G|,$$

which coincides with the lower bound derived in (18). This gives the formula of Theorem 2.4. $\square$

Let us finish with a remark. Keeping the same notation, we may observe that r being fixed ($\leq k+l$), the ratio

$$\frac{(m-r+k+l)|G|}{m(k+l)} = \frac{|G|}{k+l} + \frac{(k+l-r)|G|}{m(k+l)}$$

is a decreasing function of m. It follows that among the divisors of $\exp(G)$ with the same value modulo $k+l$, m is *minimal*.

5.4. The case of cyclic groups (proof of Theorem 2.6)

We start with a general remark. If d is congruent to 1 modulo $k+l$ then

$$\frac{[(d-2)/(k+l)]+1}{d}=\frac{d-1}{(k+l)d}=\frac{1}{k+l}-\frac{1}{(k+l)d}$$

which is both less than $1/(k+l)$ and an increasing function of d. Otherwise, that is, if d is not congruent to 1 modulo $k+l$, then

$$\frac{[(d-2)/(k+l)]+1}{d}\geq\frac{1}{k+l}$$

as shown by formula (19).

Proof of Theorem 2.6. Suppose first that n has at least one divisor not congruent to 1 modulo $k+l$. In this case, we apply Theorem 2.4 and the conclusion follows since $\exp(\mathbb{Z}/n\mathbb{Z})=n$.

Suppose now that any divisor d of n is congruent to 1 modulo $k+l$. In particular, n must be odd. We can apply successively Theorem 2.3 and Lemma 5.8. This gives

$$\max_{d|n}\left(\frac{\left[\frac{d-2}{k+l}\right]+1}{d}\right)n\leq\lambda_{k,l}(\mathbb{Z}/n\mathbb{Z})\leq\max\left(\frac{n-1}{k+l},\max_{d|n}\left(\frac{\left[\frac{d-2}{k+l}\right]+1}{d}\right)n\right). \tag{20}$$

But the general remark stated above shows that

$$\max_{d|n}\left(\frac{[(d-2)/(k+l)]+1}{d}\right)n=\max_{d|n}\frac{(d-1)n}{(k+l)d}=\frac{n-1}{k+l}.$$

So, putting this in (20) gives the result. □

6. Sum-free sets revisited

We now apply the structural result obtained in Section 4 (Theorem 2.2) to sum-free sets. What we obtain is the following improvement on Yap's results since we characterize *all* maximal sum-free subsets with cardinality at least one third of that of the ambient group, generalizing Theorems 7.8 and 7.9 of [28]. As a by-product, this gives an alternative proof of Yap's result that we write down completely here for the sake of both clarity and completeness.

Proposition 6.1. *Let G be any finite Abelian group. The maximal sum-free sets with cardinality larger than or equal to $(|G|+1-\epsilon(G))/3$ are exactly the arithmetic progressions of cosets $\psi^{-1}_{G,G/H}(\mathcal{C})$, where H is any subgroup of G such that G/H is cyclic, and*

- *if $|G|$ is even: $|G/H| \equiv 2 \pmod 3$, and $\mathcal{C} \subset G/H$ is the non-zero element if $|G/H| = 2$ and any element of $\mathcal{GP}_{2,1}(G/H)$ if $|G/H| \geq 5$,*
- *if $|G|$ is odd: $|G/H| \equiv 0$ or $2 \pmod 3$, and $\mathcal{C} \subset G/H$ is one of the two non-zero elements if $|G/H| = 3$ and any element of $\mathcal{GP}_{2,1}(G/H)$ if $|G/H| \geq 5$.*

Proof. We will prove Proposition 6.1 in the following equivalent form: *the maximal sum-free sets with cardinality larger than or equal to $(|G|+1-\epsilon(G))/3$ are exactly the following:*

if $|G|$ is even:

(i) *$G \setminus H$, where H is any subgroup of G with order $|G|/2$,*

(ii) *the set $\psi^{-1}_{G,G/H}(\mathcal{C})$, where H is any subgroup of G such that G/H is cyclic, $|G/H| \equiv 2 \pmod 3$, $|G/H| \geq 5$ and where $\mathcal{C}$ is any element of $\mathcal{GP}_{2,1}(G/H)$,*

and if $|G|$ is odd:

(iii) *one of the two H-cosets different from H, where H is any subgroup of G with order $|G|/3$,*

(iv) *the set $\psi^{-1}_{G,G/H}(\mathcal{C})$, where H is any subgroup of G such that G/H is cyclic, $|G/H| \not\equiv 1 \pmod 3$, $|G/H| \geq 5$ and where $\mathcal{C}$ is any element of $\mathcal{GP}_{2,1}(G/H)$.*

Any of these kinds of sets is a maximal sum-free set. For (i) and (iii), this is easily seen directly. For (ii) and (iv), this follows from Lemmas 5.7 and 4.1 (in the special case $k = 2, l = 1$).

Let us check that they all have a cardinality larger than or equal to $(|G| + 1 - \epsilon(G))/3$. Cases (i) and (iii) are immediate (recall that $\epsilon(G) = 1$ is equivalent to $|G|$ odd). Cases (ii) and (iv) follow from

$$|\psi^{-1}_{G,G/H}(\mathcal{C})| = |\mathcal{C}||H| = \gamma_{2,1}(G/H)|H| = \left(\left\lceil \frac{|G/H| - 2}{3} \right\rceil + 1 \right) |H|.$$

In case (ii), this is $(|G| + |H|)/3$ while, in case (iv), this is at least $|G|/3$. In both cases, this is larger than or equal to $(|G| + 1 - \epsilon(G))/3$, as wished.

Conversely, there remains to show that there are no other solutions. Take a maximal sum-free set $\mathcal{A}$ such that

$$|\mathcal{A}| \geq \frac{|G| + 1 - \epsilon(G)}{3}. \tag{21}$$

We distinguish two cases.

We assume first that $\mathcal{A}$ is included in a coset $a + H$ (for some proper subgroup H of G). If $(k-l)a \in H$, by (1), $|\mathcal{A}| \leq |H|/2 \leq |G|/4$ which is in contradiction with (21). Therefore, ka and la are not in the same H-coset. The maximality of $\mathcal{A}$ then implies $\mathcal{A} = a + H$ and subsequently $|\mathcal{A}| = |H|$. Considering (21) shows that, if $|G|$ is even, then the only possible case is $|H| = |G|/2$ which leads to case (i). If $|G|$ is odd then (21) shows that the only possibility is $|H| = |G|/3$ which leads to case (iii). This closes the first case considered.

We now assume that $\mathcal{A}$ is not contained in any proper coset. By (21), we may apply Theorem 2.2: there is a subgroup H of G such that $\mathcal{A} + H = \mathcal{A}$, G/H is a cyclic group and $\mathcal{A}/H$ is an arithmetic progression and a maximal sum-free set. We put $q = |G/H|$, thus G/H is isomorphic to the cyclic group $\mathbb{Z}/q\mathbb{Z}$. Clearly, $q > 1$.

By Lemma 5.5, since $\mathcal{A}/H$ is a non-empty maximal (k,l)-free arithmetic progression in $\mathbb{Z}/q\mathbb{Z}$ and $\mathcal{A}/H$ is not contained in any proper coset in G/H (otherwise $\mathcal{A}$ itself would be contained in a proper coset), we obtain $q \geq 5$ and

$$|\mathcal{A}| = |\mathcal{A}/H|\ |H| \leq \gamma_{2,1}(q)|H| = \left(\left\lceil \frac{q-2}{3} \right\rceil + 1\right)\frac{|G|}{q}. \tag{22}$$

The case $q \equiv 1 \pmod 3$ is readily seen to be in contradiction with (21).

If $q \equiv 0 \pmod 3$, (21) and (22) show that

$$\frac{|G| + 1 - \epsilon(G)}{3} \leq |\mathcal{A}| = |\mathcal{A}/H|\ |H| \leq \gamma_{2,1}(q)|H| = \frac{|G|}{3}.$$

This implies that $\epsilon(G) = 1$ (that is, G has an odd cardinality), $|\mathcal{A}| = |G|/3$ and $|\mathcal{A}/H| = \gamma_{2,1}(q)$.

If $q \equiv 2 \pmod 3$, we obtain

$$\frac{|G| + 1 - \epsilon(G)}{3} \leq |\mathcal{A}/H|\ |H| \leq \gamma_{2,1}(q)|H| = \left(\frac{q+1}{3}\right)\frac{|G|}{q}. \tag{23}$$

In fact, once again, one has $|\mathcal{A}/H| = \gamma_{2,1}(q)$ because otherwise (23) yields

$$\frac{|G|}{3} \leq |\mathcal{A}/H|\ |H| \leq (\gamma_{2,1}(q) - 1)|H| = \left(\frac{q-2}{3q}\right)|G| < \frac{|G|}{3},$$

a contradiction.

In both cases, $\mathcal{A}/H$ must have cardinality $\gamma_{2,1}(q)$ which implies $\mathcal{A}/H$ to be an element of $\mathcal{GP}_{2,1}(G/H)$. This achieves the proof. □

Since this lemma gives a complete description of "large" maximal sum-free sets, it could reveal useful for the problem of counting the number of sum-free sets in finite Abelian groups [1, 17].

Acknowledgements. We are grateful to an anonymous referee whose remarks helped us to improve the presentation of this paper.

References

[1] N. Alon, Independent sets in regular graphs and sum-free subsets of finite groups, *Israel J. Math.* **73** (1991), 247–256.

[2] T. Bier and A. Y. M. Chin, On (k,l)-sets in cyclic groups of odd prime order, *Bull. Austral. Math. Soc.* **63** (2001), 115–121.

[3] P. J. Cameron and P. Erdős, Notes on sum-free and related sets, Recent trends in combinatorics (Mátraháza, 1995), *Combin. Probab. Comput.* **8** (1999), 95–107.

[4] A. L. Cauchy, Recherches sur les nombres, *J. École Polytech.* **9** (1813), 99–123.

[5] H. Davenport, On the addition of residue classes, *J. London Math. Soc.* **10** (1935), 30–32.
[6] H. Davenport, A historical note, *J. London Math. Soc.* **22** (1947), 100–101.
[7] P. H. Diananda and H. P. Yap, Maximal sum-free sets of elements of finite groups, *Proc. Japan Acad.* **45** (1969), 1–5.
[8] Y. ould Hamidoune, Sur les atomes d'un graphe orienté, *C.R. Acad. Sci. Paris* **284** (1977), 1253–1256.
[9] Y. ould Hamidoune, An isoperimetric method in Additive Theory, *J. Algebra* **179** (1996), 622–630.
[10] Y. ould Hamidoune, Subsets with small sums in Abelian groups I: the Vosper property, *Europ. J. of Combinatorics* **18** (1997), 541–556.
[11] Y. ould Hamidoune, Some results in additive number theory I: The critical pair theory, *Acta Arith.* **XCVI.2** (2001), 97–119.
[12] Y. ould Hamidoune and A. Plagne, A generalization of Freiman's $3k-3$ theorem, *Acta Arith.* **CIII** (2002), 147–156.
[13] Y. ould Hamidoune and A. Plagne, A multiple set version of the $3k-3$ theorem, *Rev. Mat. Iberoam.*, to appear.
[14] Y. ould Hamidoune and Ø. J. Rødseth, An inverse theorem mod p, *Acta Arith.* **XCII.3** (2000), 251–262.
[15] J. H. B. Kemperman, On small sumsets in Abelian groups, *Acta Math.* **103** (1960), 66–88.
[16] M. Kneser, Abschätzung der asymptotischen Dichte von Summenmengen, *Math. Z.* **58** (1953), 459–484.
[17] V. F. Lev, T. Łuczak and T. Schoen, Sum-free sets in Abelian groups, *Israel J. Math.* **125** (2001), 347–367.
[18] H. B. Mann, *Addition Theorems: the Addition Theorems of Group Theory and Number Theory*, Interscience Tracts in Pure and Applied Mathematics **18**, John Wiley, 1965.
[19] M. B. Nathanson, *Additive number theory: Inverse problems and the geometry of sumsets*, Graduate Texts in Mathematics **165**, Springer-Verlag, 1996.
[20] J. E. Olson, On the sum of two sets in a group, *J. Number Theory* **18** (1984), 110–120.
[21] A. Plagne, Maximal (k,l)-free sets in $\mathbb{Z}/p\mathbb{Z}$ are arithmetic progressions, *Bull. Austral. Math. Soc.* **65** (2002), 137–144.
[22] A. H. Rhemtulla and A. P. Street, Maximal sum-free sets in finite Abelian groups, *Bull. Austral. Math. Soc.* **2** (1970), 289–297.
[23] P. Samuel, *Théorie algébrique des nombres*, Hermann, 1967.
[24] A. P. Street, Maximal sum-free sets in cyclic groups of prime-power order, *Bull. Austral. Math. Soc.* **4** (1971), 407–418.
[25] A. P. Street, Maximal sum-free sets in Abelian groups of order divisible by three, *Bull. Austral. Math. Soc.* **6** (1972), 439–441.
[26] A. G. Vosper, The critical pairs of subsets of a group of prime order, *J. London Math. Soc.* **31** (1956), 200–205.
[27] A. G. Vosper, Addendum to "The critical pairs of subsets of a group of prime order", *J. London Math. Soc.* **31** (1956), 280–282.
[28] W. D. Wallis, A. P. Street and J. S. Wallis, *Combinatorics: Room squares, sum-free sets, Hadamard matrices*, Lecture Notes in Mathematics **292**, Springer-Verlag, 1972.
[29] H. P. Yap, Maximal sum-free sets of group elements, *J. London Math. Soc.* **44** (1969), 131–136.
[30] H. P. Yap, Structure of maximal sum-free sets in C_p, *Acta Arith.* **XVII** (1970), 29–35.
[31] H. P. Yap, Maximal sum-free sets in finite abelian groups, *Bull. Austral. Math. Soc.* **4** (1971), 217–223.
[32] H. P. Yap, Maximal sum-free sets in finite abelian groups, II, *Bull. Austral. Math. Soc.* **5** (1971), 43–54.
[33] H. P. Yap, Maximal sum-free sets in finite abelian groups, III, *J. Number Theory* **5** (1973), 293–300.

[34] H. P. Yap, Maximal sum-free sets in finite abelian groups IV, *Nanta Math.* **5** (1972), 70–75.
[35] H. P. Yap, Maximal sum-free sets in finite abelian groups, V, *Bull. Austral. Math. Soc.* **13** (1975), 337–342.

Yahya ould Hamidoune
CNRS et Équipe Combinatoire
Université Pierre et Marie Curie
Case 189
4 place Jussieu
75005 Paris
France
e-mail: yha@ccr.jussieu.fr

Alain Plagne
LIX
École polytechnique
91128 Palaiseau Cedex
France
e-mail: plagne@lix.polytechnique.fr

(Received: June 10, 2002; revised version: March 17, 2003)