Problems in additive number theory

by

Željka Ljujić

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York

2011

This manuscript has been read and accepted for the Graduate Faculty in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

Professor Melvyn B. Nathanson

Date	Chair of Examining Commitee

Professor Józef Dodziuk

Date	Executive Officer

Professor Melvyn B. Nathanson

Professor Kevin O'Bryant

Professor Mark Sheingorn

Supervisory Commitee

The City University of New York

Abstract

PROBLEMS IN ADDITIVE NUMBER THEORY by

Željka Ljujić

Advisor: Professor Melvyn B. Nathanson

In the first chapter we obtain the Biro-type upper bound for the smallest period of B in the case when A is a finite multiset of integers and B is a multiset such that A and B are t-complementing multisets of integers. In the second chapter we answer an inverse problem for lattice points proving that if $K \subseteq \mathbb{R}^2$ is a compact set such that $K + \mathbb{Z}^2 = \mathbb{R}^2$ then the integer points of the difference set of K, $(K - K) \cap \mathbb{Z}^2$, is not contained on the coordinate axes, $\mathbb{Z} \times \{0\} \cup \{0\} \times \mathbb{Z}$. In the third chapter we show that there exist infinite sets A and M of positive integers whose partition function $p_{A,M}$ has weakly superpolynomial but not superpolynomial growth. The last chapter deals with the size of a sum of dilates $2 \cdot A + k \cdot A$. We prove that if k is a power of an odd prime or product of two primes and A a finite set of integers such that $|A| > 8k^k$, then $|2 \cdot A + k \cdot A| \geq (k+2)|A| - k^2 - k + 2$.

Contents

List of Figures

Chapter 1

Periodicity of complementing multisets

The content of this chapter has been accepted for publication in Functiones et Approximatio Commentarii Mathematici, [15].

Let A and B be subsets of integers. The sumset $A + B$ is the set of all integers of the form $a + b$, where $a \in A$ and $b \in B$. If every integer has a unique representation as the sum of an element of A and an element of B, then we write $A \oplus B = \mathbb{Z}$ and we say that A and B are *complementing sets of integers*.

Let A be a finite set of integers. One of the classical problems is to decide whether there exists an infinite set B such that $A \oplus B = \mathbb{Z}$.

We say that a set $B \subset \mathbb{Z}$ is *periodic* if there exists $k \in \mathbb{Z}_{>0}$ such that $B + \{k\} = B$. In that case, we say that k is a *period* of B. An early result of D.J. Newman [26] states the following:

Theorem 1 (D.J. Newman [26]). *Let A be a nonempty finite set of integers and let $diam(A) = \max(A) - \min(A)$. If there exists a set B such that $A \oplus B = \mathbb{Z}$, then B is periodic with period*

$$k \leq 2^{diam(A)}.$$

From here, one can ask a natural question: What is the best upper bound for the period in terms of $\mathrm{diam}(A)$? I.Z. Ruzsa, [in Tijdeman [29], Appendix], translated the problem into a problem of divisibility of certain integer polynomials and proved

$$\log k << \sqrt{\mathrm{diam}(A) \log(\mathrm{diam}(A))}.$$

M. Koloutzakis [16] obtained a slightly weaker bound using the same method. A. Biro [2], improved the Ruzsa's result on the divisibility of integer polynomials and obtained the following bound.

Theorem 2 (A. Biró [2]). *For every $\varepsilon > 0$ there exists an integer n_0 with the following property: Let A and B be sets of integers such that A is finite and $A \oplus B = \mathbb{Z}$. Then, if $diam(A) \geq n_0$, there exists a period k of B such that*

$$\log k \leq diam(A)^{\frac{1}{3}+\epsilon}.$$

The problem of complementing sets of integers was generalized to linear

forms by M.B. Nathanson [25] as follows: we consider two linear forms

$$\psi(x_1, \ldots, x_h) = u_1 x_1 + \cdots + u_h x_h$$

and

$$\rho(x_1, \ldots, x_h, y) = \psi(x_1, \ldots, x_h) + vy,$$

with nonzero integer coefficients $u_1, \ldots, u_h, v$. Let $\mathcal{A} = (A_1, \ldots, A_h)$ be an h-tuple of nonempty finite sets of integers and B a set of integers. We introduce the sets

$$\psi(\mathcal{A}) = \{u_1 a_1 + \cdots + u_h a_h : a_i \in A_i\}$$

and

$$\rho(\mathcal{A}, B) = \{u_1 a_1 + \cdots + u_h a_h + vb : a_i \in A_i, b \in B\}.$$

We denote $\mathrm{diam}(\psi(\mathcal{A})) = \max(\psi(\mathcal{A})) - \min(\psi(\mathcal{A}))$.

For every integer n, we define the representation function associated to ψ

$$R_{\mathcal{A}}^{(\psi)}(n) = \mathrm{card}(\{(a_1, \ldots, a_h) \in A_1 \times \cdots \times A_h : \psi(a_1, \ldots, a_h,) = n\}),$$

and the representation function associated to ρ by

$$R_{\mathcal{A},B}^{(\rho)}(n) = \mathrm{card}(\{(a_1, \ldots, a_h, b) \in A_1 \times \cdots \times A_h \times B : \rho(a_1, \ldots, a_h, b) = n\}).$$

We say that $\mathcal{A}$ and B are *complementing sets of integers with respect to the linear form* ρ if $\rho(\mathcal{A}, B) = \mathbb{Z}$ and $R_{\mathcal{A},B}^{(\rho)}(n) = 1$, for all integers n. Similarly, $\mathcal{A}$ and B are *t-complementing sets of integers with respect to* ρ if $\rho(\mathcal{A}, B) = \mathbb{Z}$ and $R_{\mathcal{A},B}^{(\rho)}(n) = t$, for all integers n.

Theorem 3 (M.B. Nathanson [25]). *Let $h \geq 1$ and let*

$$\rho(x_1, \ldots, x_h, y) = \psi(x_1, \ldots, x_h) + vy$$

be a linear form with nonzero integer coefficients $u_1, \ldots, u_h, v$. Let $\mathcal{A} = (A_1, \ldots, A_h)$ be an h-tuple of nonempty finite sets of integers. If $\mathcal{A}$ and B are t-complementing sets of integers with respect to ρ, then B is periodic with period

$$k \leq 2^{\frac{diam(\psi(A))}{|v|}}.$$

Here, we consider the complementing multisets of integers. More precisely, let S be a multiset of integers. For each integer n, we denote by $w_S(n) \in \mathbb{Z}_{\geq 0}$ the weight of n in S, which is the number of occurrences of n in S. Let A be a finite multiset of integers and let B be a multiset of integers. For every integer n, we define the representation function associated to the multisets A and B as

$$R_{A,B}(n) = \sum_{\substack{n=a+b \\ a \in A, b \in B}} w_A(a) w_B(b).$$

Let $t \in \mathbb{Z}_{>0}$. We say that A and B are *t-complementing multisets of integers* if $A + B = \mathbb{Z}$ and $R_{A,B}(n) = t$, for all $n \in \mathbb{Z}$. In that case, we write $A \oplus_t B = \mathbb{Z}$.

We say that a multiset B is *periodic* if there exists $k \in \mathbb{Z}_{>0}$ such that $w_B(n+k) = w_B(n)$, for all $n \in \mathbb{Z}$. Any such k is called a *period* of a multiset B. More generally, we say that a multiset of integers B is *eventually periodic* if there exist $k \in \mathbb{Z}_{>0}$ and $n_0 \in \mathbb{Z}$ such that if $n \geq n_0$, then $w_B(n+k) = w_B(n)$. In that case, k is an *eventual period* of B.

Similarly, a representation function $R_{A,B}$ is *eventually periodic* if there exist $m \in \mathbb{Z}_{>0}$ and $n_0 \in \mathbb{Z}$ such that if $n \geq n_0$ we have $R_{A,B}(n+m) = R_{A,B}(n)$. An integer m is called an *eventual period* of $R_{A,B}$.

Note that in the case $t = 1$ the multisets A and B are an ordinary sets and the problem of complementing multisets becomes the classical problem of complementing sets of integers. In the case of complementing sets with respect to linear forms, we can consider $\psi(\mathcal{A})$ as a multiset A'. More precisely, if $r = u_1a_1 + \cdots + u_ha_h \in \psi(\mathcal{A})$, we define $w_{\psi(\mathcal{A})}(r) = R_{\mathcal{A}}^{(\psi)}(r)$. Then, if there exists a set B such that $\mathcal{A}$ and B are t-complementing sets of integers with respect to ρ, we have that $A' \oplus_t B' = \mathbb{Z}$, where $B' = vB$ and B is periodic with period k if and only if B' is periodic with period vk.

We prove the following equivalent of Theorem 1 [D.J. Newman [26]] in the case of multisets:

Theorem 4. *Let A be a nonempty finite multiset of integers. Let $diam(A) = \max(A) - \min(A)$. If there exists a multiset B such that $A \oplus_t B = \mathbb{Z}$, then B is periodic with period*

$$k \leq (t+1)^{diam(A)}.$$

Moreover, we follow Ruzsa's idea and translate the problem into the problem of the divisibility of integer polynomials. We extend the main theorem in [2] to fit our purpose and we obtain the following theorem.

Theorem 5. *For every $\varepsilon > 0$ there exists an integer n_0 with the following property: Let A be a finite multiset of integers such that $|A| > 1$. Suppose*

that B is an eventually periodic infinite multiset of integers with eventual period k, and that the representation function $R_{A,B}$ is eventually periodic with eventual period m. If $n = diam(A) + m \geq n_0$ and $\sum_{a \in A} w_A(a) \leq n^c$, where $c < 100 \log 2 - 2$, then there exists an eventual period k of B such that

$$\log k \leq n^{\frac{1}{3}+\varepsilon}.$$

As an immediate corollary, we obtain a new upper bound of the period of t-complementing multisets of integers.

Theorem 6. *For every $\varepsilon > 0$ there exists an integer n_0 with the following property: Let A be a nonempty finite multiset of integers and let $diam(A) = \max(A) - \min(A)$. We assume that $diam(A) \geq n_0$ and that $\sum_{a \in A} w_A(a) \leq (diam(A)+1)^c$, where $c < 100 \log 2 - 2$. If B is a multiset such that $A \oplus_t B = \mathbb{Z}$, then B is periodic with period*

$$\log k \leq (diam(A) + 1)^{\frac{1}{3}+\varepsilon}.$$

The last theorem can be restated in terms of complementing sets of integers with respect to linear forms.

Theorem 7. *For every $\varepsilon > 0$ there exists an integer n_0 with the following property: Let $h \geq 1$ and let*

$$\rho(x_1, \ldots, x_h, y) = \psi(x_1, \ldots, x_h) + vy$$

be a linear form with nonzero integer coefficients $u_1, \ldots, u_h, v$. Let $\mathcal{A} = (A_1, \ldots, A_h)$ be an h-tuple of nonempty finite sets of integers and let

$$diam(\psi(A)) = \max(\psi(\mathcal{A})) - \min(\psi(\mathcal{A})).$$

We assume that $diam(\psi(A)) \geq n_0$ *and that* $\prod_{i=1}^{h} |A_i| \leq n^c$, *where* $c < 100 \log 2 - 2$. *If* B *is a set such that* $\mathcal{A}$ *and* B *are* t*-complementing sets of integers with respect to* ρ, *then* B *is periodic with period*

$$\log k \leq (diam(\psi(A)) + 1)^{\frac{1}{3}+\varepsilon}.$$

1.1 Preliminaries

We start by introducing some notation. Let $n \in \mathbb{Z}_{>0}$.

If p is a prime number such that $p^r | n$, but $p^{r+1} \nmid n$, for some $r \in \mathbb{Z}_{\geq 1}$, we write $p^r \parallel n$.

The set of all primitive n-th roots of unity will be denoted by μ_n. Then $\phi(x) = |\mu_n|$ denotes Euler's function and $\Phi_n(x) = \prod_{\xi \in \mu_n}(x - \xi)$ denotes the n-th cyclotomic polynomial. The number of divisors of n will be denoted by $\tau(n)$ and the number of distinct prime divisors of n by $\omega(n)$. We denote the Möbius function by $\mu(n)$.

If $f(x) = \sum a_i x^i \in \mathbb{Z}[x]$, then $\|f(x)\| = \sum |a_i|$. It is easy to see that if $f_1, f_2 \in \mathbb{Z}[x]$, then $\|f_1(x) f_2(x)\| \leq \|f_1(x)\| \|f_2(x)\|$.

As usual, log will denote the natural logarithm.

The following three lemmas are Lemma 1, Lemma 2 and Lemma 3 from [2].

Lemma 8. *Let* $f(x) \in \mathbb{C}[x]$ *be a nonzero polynomial such that* $x^d - 1 | f(x)$, *for some* $d \in \mathbb{Z}_{>0}$. *Let* $n = \deg f(x)$ *let* $g(x) = \frac{f(x)}{x^d - 1}$. *Then*

$$\|g(x)\| \leq n \|f(x)\|.$$

Lemma 9. *Let $\varepsilon > 0$ and let $f(x) \in \mathbb{C}[x]$ be a nonzero polynomial such that $\deg f(x) \leq n$, where $n \geq n_0(\varepsilon)$. Let m be a positive integer satisfying $\Phi_m(x) | f(x)$, and let $g(x) = \frac{f(x)}{\Phi_m(x)}$. Then*

$$\|g(x)\| \leq e^{n^{\varepsilon}} \|f(x)\|.$$

Lemma 10. *Let $\varepsilon > 0$ and let K be a real number such that $K \geq K_0(\varepsilon)$. Set $C = 10^5 \log K$. Then*

$$\sum_{r=1}^{K} C^{\omega(r)} \leq K^{1+\epsilon}.$$

The following lemma is a generalization of Lemma 4 in [2].

Lemma 11. *Let $f(x) \in \mathbb{Z}[x]$ be such that $f(1) \neq 0$ and $\|f(x)\| \leq n^c$, where $n = \deg(f(x))$ and c is any constant such that $c < 100 \log 2 - 1$. Suppose that $\Phi_d(x)^V | f(x)$, for some $d \in \mathbb{Z}_{>0}$. Then there exists an integer $n_0 > 1$ such that $n \geq n_0$ implies $V \leq (100 \log n)^{\omega(d)}$.*

Proof. Let p be a prime number dividing d. We write $d = p^r d_1$, where $r \geq 1$ and $(p, d_1) = 1$. If U is any integer satisfying $0 \leq U \leq V$, we obtain

$$\Phi_d(x)^{V-U} | f^{(U)}(x),$$

where $f^{(U)}(x)$ denotes the U-th derivative of $f(x)$. The products

$$\prod_{\xi \in \mu_{d_1}} \Phi_d(\xi)^{V-U} \text{ and } \prod_{\xi \in \mu_{d_1}} f^{(U)}(\xi)$$

belong to the ring of integers of the number field $\mathbb{Q}(\xi_{d_1})$, where ξ_{d_1} denotes the d_1-th primitive root of unity. On the other hand, they are fixed by all

the automorphism in $\mathrm{Gal}(\mathbb{Q}(\xi_{d_1})/\mathbb{Q})$, so they belong to $\mathbb{Q}$. We obtain that $\prod_{\xi\in\mu_{d_1}} \Phi_d(\xi)^{V-U}$, $\prod_{\xi\in\mu_{d_1}} f^{(U)}(\xi) \in \mathbb{Z}$, and

$$\left(\prod_{\xi\in\mu_{d_1}} \Phi_d(\xi)\right)^{V-U} \Bigg| \prod_{\xi\in\mu_{d_1}} f^{(U)}(\xi).$$

We denote $N = \prod_{\xi\in\mu_{d_1}} f^{(U)}(\xi)$. We have that $|f^U(\xi)| \leq \|f^{(U)}(x)\| \leq n^U\|f(x)\| \leq n^{U+c}$, so we obtain

$$|N| \leq (n^{U+c})^{\phi(d_1)}. \tag{1.1}$$

On the other hand,

$$\prod_{\xi\in\mu_{d_1}} \Phi_d(\xi) = \prod_{\xi_1,\xi_2\in\mu_{d_1}} \prod_{\eta\in\mu_{p^r}} (\xi_1 - \xi_2\eta).$$

The $\xi_1 = \xi_2$ part of the right-hand side is

$$\prod_{\xi\in\mu_{d_1}} \xi \prod_{\eta\in\mu_{p^r}} (1-\eta) = \prod_{\xi\in\mu_{d_1}} \Phi_{p^r}(1)\xi = p^{\phi(d_1)} \prod_{\xi\in\mu_{d_1}} \xi.$$

Hence,

$$(p^{\phi(d_1)})^{V-U} | N.$$

Hence, if $N \neq 0$, we have $(p^{V-U})^{\phi(d_1)} \leq |N|$. Using (1.1), we obtain

$$p^{V-U} \leq n^{U+c}.$$

Now, let us assume that $V \geq 100\log n$. Let U be such that $0 \leq U \leq \frac{V}{100\log n}$. We have

$$\begin{aligned} 2^{V(1-\frac{1}{100\log n})} \leq 2^{V-U} \leq p^{V-U} \leq n^{U+c} &\leq n^{\frac{V}{100\log n}} n^c \\ &= e^{\frac{V}{100}} n^c \leq e^{(c+1)\frac{V}{100}}, \end{aligned}$$

so

$$e^{V(1-\frac{1}{100\log n})\log 2} \leq e^{(c+1)\frac{V}{100}}$$

has to be satisfied. This is equivalent to

$$\frac{\log 2}{\log n} + c \geq 100\log 2 - 1.$$

But $c < 100\log 2 - 1$, so there exists n_0 such that if $n \geq n_0$ the last inequality doesn't hold, hence $N = 0$. This implies that if $n \geq n_0$ and $V \geq 100\log n$, we have $\prod_{\xi\in\mu_{d_1}} f^{(U)}(\xi) = 0$, for all $0 \leq U \leq \frac{V}{100\log n}$. Hence if $n \geq n_0$ and $V \geq 100\log n$, we have

$$\Phi_{d_1}(x)^{U+1} | f(x),$$

for all $0 \leq U \leq \frac{V}{100\log n}$.

Let $d = p_1^{r_1}\cdots p_k^{r_k}$, where p_i are distinct prime numbers and $r_i > 0$ for all i. We repeat the step above $k = \omega(d)$ times. We obtain that if $V > (100\log n)^{\omega(d)}$, then $f(1) = 0$, a contradiction. □

We present the proof of the generalization of the main theorem in [2]. Throughout the proof we will follow Biro's argument.

Theorem 12. *For every $\varepsilon > 0$ there exists an integer n_0 with the following property: Let $q(x) \in \mathbb{Z}[x]$. Assume that there is a polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(1) \neq 0$ and there exists a positive integer m such that $q(x)$ divides $(x^m - 1)f(x)$. Let us denote by n the degree of polynomial $(x^m-1)f(x)$ and assume that $n \geq n_0$. If $\|f(x)\| \leq n^c$, where c is any constant such that $c < 100\log 2 - 2$ and there exists a positive integer k such that $q(x)$*

divides $l(x^k - 1)$, for some integer l, then for the smallest such k we have

$$\log k \leq n^{1/3+\varepsilon}$$

Proof. Let $q(x) \mid l(x^{k'} - 1)$, for some $k', l \in \mathbb{Z}$. Then

$$q(x) = l' \prod_{d \in D} \Phi_d(x),$$

where $l' \in \mathbb{Z}$ such that $l'|l$ and D is a set of some divisors of k'. If we set $k = \operatorname{lcm}\{d \mid d \in D\}$, we will obtain

$$q(x) \mid l(x^k - 1).$$

Our aim is to give an upper bound for k.

On the other hand,

$$\deg(q(x)) = \sum_{d \in D} \phi(d) \leq n. \tag{1.2}$$

Let M be an integer and L any real number satisfying

$$n^{\frac{1}{3}} < M < \frac{1}{2} n^{\frac{1}{2}},\ L > 2n^{\frac{1}{2}}.$$

In order to estimate k, we will estimate the products of prime factors of k.

Case 1. Let p be a prime such that $p^r \parallel k$, for some $r \geq 1$ and $p^r \geq L$. Then $p^r|d$, for some $d \in D$. Moreover, every such p^r divides a different $d \in D$, since otherwise we would have

$$\phi(d) \geq \phi(p_1^{r_1})\phi(p_2^{r_2}) \geq (\frac{1}{2}p_1^{r_1})(\frac{1}{2}p_2^{r_2}) \geq \frac{L^2}{4} > n,$$

which would contradict (1.2). We obtain

$$\frac{1}{2}\sum_{\substack{p^r\|k\\ p^r\geq L}} L \leq \frac{1}{2}\sum_{\substack{p^r\|k\\ p^r\geq L}} p^r \leq \sum_{\substack{p^r\|k\\ p^r\geq L}} \phi(p^r) \leq \sum_{d\in D}\phi(d) \leq n.$$

Moreover, for every such p^r we have $p^r \leq 2n$, and the number of such prime powers is at most $\frac{2n}{L}$, so

$$\prod_{\substack{p^r\|k\\ p^r\geq L}} p^r \leq (2n)^{\frac{2n}{L}}. \tag{1.3}$$

Case 2. Let p be a prime such that $p^r \parallel k$, for some $r \geq 1$ and $p^r \leq M$.

$$\prod_{\substack{p^r\|k\\ p^r\leq M}} p^r \leq \prod_{p^r\leq M} p^r \leq e^{c_1 M}. \tag{1.4}$$

Case 3. Let p be a prime such that $p^r \parallel k$, for some $r \geq 2$ and $M < p^r < L$. Similarly as in the previous case, we obtain

$$\prod_{\substack{p^r\|k\\ M<p^r<L, r\geq 2}} p^r \leq \prod_{p^r<L, r\geq 2} p^r \leq e^{c_2\sqrt{L}}. \tag{1.5}$$

Case 4. Let p be a prime such that $p \parallel k$ and $M < p < L$. We need to estimate

$$\prod_{\substack{p\|k\\ M<p<L}} p.$$

Every such p divides a $d \in D$, but a given $d \in D$ is divisible by at most two such primes, since otherwise we would have

$$\phi(d) \geq \phi(p_1)\phi(p_2)\phi(p_3) \geq (p_1-1)(p_2-1)(p_3-1) \geq M^3 > n,$$

which would contradict (1.2). Similarly, if $d \in D$ is divisible by two such primes, we have $\phi(d) \geq M^2$, so the number of primes $p \parallel k$ with $M < p < L$ for which there is another such prime p' and a $d \in D$ with $p, p' | d$, is at most $\frac{2n}{M^2}$. Whence,

$$\prod_{\substack{p \parallel k \\ M<p<L}} p \leq L^{\frac{2n}{M^2}} \prod_{p \in \mathcal{P}} p,$$

where $\mathcal{P} \subseteq \{p \parallel k \mid M < p < L\}$ is such that each $d \in D$ is divisible by at most one $p \in \mathcal{P}$.

We obtain that for every $p \in \mathcal{P}$ there is a $d_p \in D$ such that $p | d_p$ and if $p_1, p_2 \in \mathcal{P}$ are two distict primes then $d_{p_1} \neq d_{p_2}$. By (1.2), $\sum_{p \in \mathcal{P}} \phi(d_p) \leq n$.

On the other hand, if $p \in \mathcal{P}$, then $p \parallel k$, whence $p \parallel d_p$ and

$$\phi(d_p) = (p-1)\phi\left(\frac{d_p}{p}\right) \geq c_3(\varepsilon) M \left(\frac{d_p}{p}\right)^{1-\varepsilon}.$$

Let K be a real number. Then, if $p \in \mathcal{P}$ and $\frac{d_p}{p} \geq K$ we will have $\phi(d_p) \geq c_3(\epsilon) M K^{1-\epsilon}$, so the number of such primes is at most $\frac{n}{c_3(\varepsilon) M K^{1-\varepsilon}}$. Hence

$$\prod_{p \in \mathcal{P}} p \leq L^{c_4(\epsilon) \frac{n}{M K^{1-\epsilon}}} \prod_{p \in \mathcal{P}'} p, \tag{1.6}$$

where $\mathcal{P}' = \{p \in \mathcal{P} \mid 1 \leq \frac{d_p}{p} < K\}$.

We partition $\mathcal{P}'$ into subsets

$$\mathcal{P}' = \bigcup_{1 \leq r < K} \mathcal{P}_r,$$

where $\mathcal{P}_r = \{p \in \mathcal{P}' \mid \frac{d_p}{p} = r\}$.

We fix an r such that $1 \leq r < K$. Let $V_r \geq 0$ be the largest integer with the property

$$\Phi_r(x)^{V_r} \mid (x^m - 1)f(x)$$

and let

$$g(x) = \frac{(x^m - 1)f(x)}{\Phi_r(x)^{V_r}}.$$

By Lemma 9, we have

$$\|g(x)\| \leq e^{V_r n^\varepsilon} \|(x^m - 1)f(x)\| \leq 2n^c e^{V_r n^\varepsilon}.$$

Let

$$\nu = \prod_{\xi \in \mu_r} g(\xi).$$

Then $\nu \in \mathbb{Z}$, $\nu \neq 0$ and $|\nu| \leq \|g\|^{\phi(r)}$.

On the other hand, $\prod_{p \in \mathcal{P}_r} \Phi_{pr}(x) | q(x)$ and $q(x) | (x^m - 1)f(x)$, so $\prod_{p \in \mathcal{P}_r} \Phi_{pr}(x) | (x^m - 1)f(x)$. Moreover, $(\Phi_r(x), \prod_{p \in \mathcal{P}_r} \Phi_{pr}(x)) = 1$ and we obtain

$$\prod_{p \in \mathcal{P}_r} \Phi_{pr}(x) \mid g(x).$$

Hence,

$$\prod_{p \in \mathcal{P}_r} \Big(\prod_{\xi \in \mu_r} \Phi_{pr}(\xi) \Big) \mid \nu.$$

For every $p \in \mathcal{P}_r$, we have $(p, r) = 1$, so

$$\prod_{\xi \in \mu_r} \Phi_{pr}(\xi) = \prod_{\xi_1, \xi_2 \in \mu_r} \prod_{\eta \in \mu_p} (\xi_1 - \xi_2 \eta).$$

Setting $\xi_1 = \xi_2$, we obtain that the right-hand side is divisible by $p^{\phi(r)}$. It follows that

$$\prod_{p \in \mathcal{P}_r} p^{\phi(r)} \mid \nu,$$

and

$$\prod_{p\in\mathcal{P}_r} p^{\phi(r)} \le |\nu| \le \|g(x)\|^{\phi(r)}.$$

Consequently,

$$\prod_{p\in\mathcal{P}_r} p \le \|g(x)\| \le 2n^c e^{V_r n^\varepsilon}.$$

This implies that if n is sufficiently large, we have

$$|\mathcal{P}_r| \le c_5(V_r+1)n^\epsilon,$$

so

$$\prod_{p\in\mathcal{P}'} p \le L^{c_5 n^\epsilon \sum_{1\le r<K}(V_r+1)}. \tag{1.7}$$

Combining (1.3), (1.4), (1.5), (1.6) and (1.7), we obtain that if n is sufficiently large, then

$$\begin{aligned}\log k &\le \frac{2n}{L}\log(2n) + c_1 M + c_2\sqrt{L} + c_4(\varepsilon)\frac{n}{MK^{1-\varepsilon}}\log L \\ &\qquad + c_5 n^\epsilon \sum_{1\le r<K}(V_r+1)\log L \\ &\le \frac{2n}{L}\log(2n) + c_1 M + c_2\sqrt{L} \\ &\qquad + c_6(\epsilon)(\log L)(Kn)^\epsilon\Big(\frac{n}{M^2} + \frac{n}{MK} + \sum_{1\le r<K}(V_r+1)\Big)\end{aligned}$$

The L part is optimized by taking $L = n^{\frac{2}{3}}$. Next, we estimate $V_r + 1$, using Lemma 11. Let

$$h(x) = \frac{(x^m-1)f(x)}{x-1}.$$

Then $h(x) \in \mathbb{Z}[x]$ is a nonzero polynomial such that $h(1) \neq 0$. Also, we have $\deg(h(x)) \leq n$ and $\|h(x)\| \leq m\|f(x)\| \leq n^{c+1}$, where $c < 100 \log 2 - 2$. Now, if $r > 1$, we have $\Phi_r(x)^{V_r} \mid h(x)$ and by Lemma 11, $V_r \leq (100 \log n)^{\omega(r)}$, for sufficiently large n. We obtain

$$V_r + 1 \leq (200 \log n)^{\omega(r)}, \text{ for } r > 1 \text{ and } V_1 + 1 = 2.$$

Assuming a weak estimate $K \geq n^{\frac{1}{100}}$ and using Lemma 10, we finally have

$$\log k \leq c_7(\epsilon)(Kn)^{2\epsilon}(n^{\frac{1}{3}} + M + \frac{n}{M^2} + \frac{n}{MK} + K).$$

This is nearly optimized in K by $K = (\frac{n}{M})^{\frac{1}{2}}$, and the remaining expression is nearly optimized in M with $M = n^{\frac{1}{3}}$. We fix the parameters

$$K = n^{\frac{1}{3}}, \ , M = \lfloor 2n^{\frac{1}{3}} \rfloor, \ , L = n^{\frac{2}{3}}.$$

and obtain

$$\log k \leq n^{\frac{1}{3}+10\epsilon},$$

for sufficiently large n. □

1.2 Multisets and periodicity

In this section we prove Theorem 4 and Theorem 5. Let A be a finite multiset of integers and let B be a multiset such that $A \oplus_t B = \mathbb{Z}$. We denote $\alpha = \min(A)$. We define a multiset $A' = A - \alpha = \{a - \alpha \mid a \in A\}$, with $w_{A'}(a - \alpha) = w_A(a)$ for all $a \in A$. If $n \in \mathbb{Z}$, we have

$$R_{A',B}(n) = \sum_{\substack{n=a'+b \\ a'=a-\alpha\in A', b\in B}} w_{A'}(a')w_B(b)$$
$$= \sum_{\substack{n+\alpha=a+b \\ a\in A, b\in B}} w_A(a)w_B(b) = R_{A,B}(n+\alpha).$$

Thus, $A' \oplus_t B = \mathbb{Z}$. Hence, we may assume without loss of generality that $\min(A) = 0$ and $\max(A) = d$, where $d = \mathrm{diam}(A)$.

Let $|A| = 1$. Then if $A = \{a\}$ and $A \oplus_t B = \mathbb{Z}$, we obtain that $B = \mathbb{Z}$ and $w_B(n) = \frac{t}{w_A(a)}$, for all $n \in \mathbb{Z}$. Hence, the multiset B is periodic with period $k = 1$ and the Theorem is immediately true. Thus, we may assume that $|A| > 1$ and $d \geq 1$.

We have

$$t = R_{A,B}(n) = \sum_{a\in A} w_A(a)w_B(n-a)$$
$$= \sum_{a\in A\setminus\{0\}} w_A(a)w_B(n-a) + w_A(0)w_B(n),$$

for all $n \in \mathbb{Z}$. Thus,

$$w_A(0)w_B(n) = t - \sum_{a\in A\setminus\{0\}} w_A(a)w_B(n-a). \tag{1.8}$$

We have that $n - d \leq n - a \leq n - 1$, for all $a \in A \setminus \{0\}$. Moreover,

$$w_A(d)w_B(n-d) = t - \sum_{a\in A\setminus\{d\}} w_A(a)w_B(n-a), \tag{1.9}$$

and $n - d + 1 \leq n - a \leq n$, for all $a \in A \setminus \{d\}$. Hence, if we know the value of w_B for any d consecutive integers, using (1.8) and (1.9) we can compute $w_B(n)$ for all integers n.

We consider the d-tuple $(w_B(i), w_B(i+1), \ldots, w_B(i+d-1))$, for some $i \in \mathbb{Z}$. Since

$$t = R_{A,B}(n+a) = \sum_{a \in A} w_A(a) w_B(n-a) \geq w_A(0) w_B(n),$$

we obtain that $w_B(n) \leq t$, for all $n \in \mathbb{Z}$. Hence,

$$(w_B(i), w_B(i+1), \ldots, w_B(i+d-1)) \in \{0, 1, \ldots, t\}^d.$$

By pigeonhole principle, there exist integers $0 \leq i < j \leq (t+1)^d$ such that

$$(w_B(i), w_B(i+1), \ldots, w_B(i+d-1)) = (w_B(j), w_B(j+1), \ldots, w_B(j+d-1)).$$

Let $k = j - i$. Then $1 \leq k \leq (t+1)^d$ and $w_B(n) = w_B(n+k)$, for $n = i, \ldots, i+d-1$. By (1.8) and (1.9), we obtain $w_B(n) = w_B(n+k)$, for all $n \in \mathbb{Z}$. This proves the Theorem 4.

Proof of the Theorem 5. As before, we may assume without loss of generality that $\min(A) = 0$ and $\max(A) = d$, where $d = \operatorname{diam}(A)$. Moreover, let $\beta \in B$. We define the mutiset $B' = B - \beta = \{b - \beta \mid b \in B\}$ with $w_{B'}(b-\beta) = w_B(b)$, for all $b \in B$. Then, $0 \in B'$ and B' is eventually periodic with eventual period k if and only if B is eventually periodic with eventual period k. If $n \in \mathbb{Z}$, we have

$$\begin{aligned} R_{A,B'}(n) &= \sum_{\substack{n=a+b' \\ a \in A, b'=b-\beta \in B'}} w_A(a) w'_B(b') \\ &= \sum_{\substack{n+\beta=a+b \\ a \in A, b \in B}} w_A(a) w_B(b) = R_{A,B}(n+\beta). \end{aligned}$$

It follows that the representation function $R_{A,B'}$ is eventually periodic with eventual period m if and only if $R_{A,B}$ is eventually periodic with eventual period m. Thus, we may assume without loss of generality that $0 \in B$.

Let

$$B^+ = \{b \in B \mid b \geq 0\}.$$

Note that if $b \in B^+$, we have that $a + b \geq 0$, for all $a \in A$. On the other hand, if $b \in B \setminus B^+$, we have $a + b < \operatorname{diam}(A)$, for all $a \in A$. Hence, $R_{A,B^+}(n) = R_{A,B}(n)$, for all $n \geq \operatorname{diam}(A)$ and R_{A,B^+} is eventually periodic with eventual period m.

We consider the generating functions

$$\lambda(x) = \sum_{a \in A} w_A(a) x^a = \sum_{n=0}^{\infty} w_A(n) x^n$$

and

$$\gamma(x) = \sum_{b \in B^+} w_B(b) x^b = \sum_{n=0}^{\infty} w_B(n) x^n.$$

Let $n_0 \in \mathbb{Z}_{>0}$ be such that $R_{A,B^+}(n+m) = R_{A,B^+}(n)$, for all integers $n \geq n_0$. Let $i_0 = \lfloor \frac{n_0}{m} \rfloor + 1$. Define $r_j = R_{A,B^+}(mi_0 + j)$ for $j = 0, 1, \ldots, m-1$. We obtain

$$\begin{aligned}
\lambda(x)\gamma(x) &= \sum_{n=0}^{\infty} R_{A,B^+}(n) x^n \\
&= \sum_{n=0}^{mi_0-1} R_{A,B^+}(n) x^n + \sum_{n=mi_0}^{\infty} R_{A,B^+}(n) x^n \\
&= \sum_{n=0}^{mi_0-1} R_{A,B^+}(n) x^n + \sum_{j=0}^{m-1} \sum_{i=i_0}^{\infty} R_{A,B^+}(mi+j) x^{mi+j}
\end{aligned}$$

$$= \sum_{n=0}^{mi_0-1} R_{A,B^+}(n)x^n + \sum_{j=0}^{m-1}\sum_{i=i_0}^{\infty} r_j x^{mi+j}$$
$$= \sum_{n=0}^{mi_0-1} R_{A,B^+}(n)x^n - \frac{1}{x^m-1}\sum_{j=0}^{m-1} r_j x^{mi_0+j}. \tag{1.10}$$

We define the polynomials

$$p_1(x) = \sum_{n=0}^{mi_0-1} R_{A,B^+}(n)x^n$$

and

$$p_2(x) = \sum_{j=0}^{m-1} r_j x^{mi_0+j}.$$

Then, using (10), we obtain

$$\lambda(x)\gamma(x) = p_1(x) - \frac{1}{x^m-1}p_2(x)$$
$$= \frac{(x^m-1)p_1(x) - p_2(x)}{x^m-1},$$

and

$$\gamma(x) = \frac{(x^m-1)p_1(x) - p_2(x)}{(x^m-1)\lambda(x)} = \frac{p(x)}{q(x)},$$

where $p(x)$ and $q(x)$ are relatively prime polynomials in $\mathbb{Z}[x]$ and $q(x)|(x^m - 1)\lambda(x)$. The multiset B^+ is eventually periodic, hence there exists $n_1 \in \mathbb{Z}_{>0}$

and $s \in \mathbb{Z}_{>0}$ such that $w_B(n+s) = w_B(n)$, for all $n \geq n_1$. Hence,

$$\begin{aligned}
(x^s-1)\gamma(x) &= (x^s-1)\sum_{n=0}^{\infty} w_B(n)x^n \\
&= \sum_{n=0}^{\infty} w_B(n)x^{n+s} - \sum_{n=0}^{\infty} w_B(n)x^n \\
&= \sum_{n=0}^{n_1-1} w_B(n)x^{n+s} + \sum_{n=n_1}^{\infty} w_B(n)x^{n+s} - \sum_{n=0}^{\infty} w_B(n)x^n \\
&= \sum_{n=0}^{n_1-1} w_B(n)x^{n+s} + \sum_{n=n_1}^{\infty} w_B(n+s)x^{n+s} - \sum_{n=0}^{\infty} w_B(n)x^n
\end{aligned}$$

$$\begin{aligned}
&= \sum_{n=0}^{n_1-1} w_B(n)x^{n+s} + \sum_{n=n_1+s}^{\infty} w_B(n)x^n - \sum_{n=0}^{\infty} w_B(n)x^n \\
&= \sum_{n=0}^{n_1-1} w_B(n)x^{n+s} - \sum_{n=0}^{n_1+s} w_B(n)x^n,
\end{aligned}$$

and $(x^s-1)\gamma(x)$ is a polynomial. Then

$$(x^s-1)\gamma(x) = \frac{(x^s-1)p(x)}{q(x)}$$

is a polynomial, whence $q(x)|(x^s-1)p(x)$. Since $\gcd(p(x), q(x)) = 1$, we conclude that there exists an integer l such that $q(x)|l(x^s-1)$. We have $\|\lambda(x)\| = \sum_{a\in A} w_A(a)$ and $\lambda(1) = \sum_{a\in A} w_A(a) \neq 0$. The conditions of Theorem 12 are fulfilled. Then there exists a positive integer k such that

$$q(x)|l'(x^k-1) \text{ for some integer } l' \text{ and } \log(k) \leq n^{\frac{1}{3}+\epsilon}.$$

It remains to prove that k is an eventual period of B^+. We have that $l'(x^k -$

$1)\gamma(x) \in \mathbb{Z}[x]$. This implies that $(x^k - 1)\gamma(x)$ is a polynomial, so

$$\begin{aligned}
(x^k - 1)\gamma(x) &= (x^k - 1)\sum_{n=0}^{\infty} w_B(n)x^n \\
&= \sum_{n=0}^{\infty} w_B(n)x^{n+k} - \sum_{n=0}^{\infty} w_B(n)x^n \\
&= \sum_{n=0}^{\infty} w_B(n)x^{n+k} - \sum_{n=n_1+k}^{\infty} w_B(n)x^n - \sum_{n=0}^{n_1+k-1} w_B(n)x^n \\
&= \sum_{n=0}^{\infty} w_B(n)x^{n+k} - \sum_{n=n_1}^{\infty} w_B(n+k)x^{n+k} - \sum_{n=0}^{n_1+k-1} w_B(n)x^n \\
&= \sum_{n=n_1}^{\infty} (w_B(n) - w_B(n+k))x^{n+k} \\
&\qquad + \sum_{n=0}^{n_1-1} w_B(n)x^{n+k} - \sum_{n=0}^{n_1+k-1} w_B(n)x^n
\end{aligned}$$

is a polynomial. Thus, there exist $n_2 \in \mathbb{Z}_{>0}$ such that $w_B(n) = w_B(n+k)$, for all $n \geq n_2$. This implies that k is an eventual period of B^+.

Chapter 2

An inverse problem for lattice points

The content of this chapter is a joint work with C. Sanabria and has been accepted for publication in Topology and its Applications, [13].

We consider the following context. Let X be a metric space which is geodesic and proper, and let Γ be a group. Let $\Gamma \times X \to X$ be a properly discontinuous action by isometries (from the left) such that the quotient $\Gamma\backslash X$ is compact. Such action is called *geometric*. The proof of the fundamental observation of geometric group theory implies that in such a context, if $K \subseteq X$ is compact fundamental domain for the Γ-action then the set

$$\{\gamma \in \Gamma |\ K \cap \gamma K \neq \emptyset\}$$

is a finite set of generators of Γ [11]. This result was proved independently by V.A. Efremovič [8], J. Milnor [17] and A. S. Švarc [28]. In the case $X = \mathbb{R}^n$ and $\Gamma = \mathbb{Z}^n$ we obtain the following theorem:

Theorem 13. *If $K \subset \mathbb{R}^n$ is a compact set such that for every $x \in \mathbb{R}^n$ there exists $y \in K$ with $x \equiv y \ (mod\ \mathbb{Z}^n)$ in $\mathbb{R}^n$, then $A = (K - K) \cap \mathbb{Z}^n$, where $K - K = \{a - b \mid a, b \in K\}$, is a finite set of generators for $\mathbb{Z}^n$.*

This result leads to the inverse problem, which was originally asked by M.B. Nathanson in [19]: If A is a finite set of generators for a group Γ, such that A is symmetric, i.e. $A^{-1} = A$, and contains the identity of Γ, does there exist a geometric action of Γ on a metric space X such that $A = \{\gamma \in \Gamma |\ K \cap \gamma K \neq \emptyset\}$ for some compact set K which is a fundamental domain for such action? In the case $X = \mathbb{R}^n$ and $\Gamma = \mathbb{Z}^n$, this problem can be translated to an inverse problem of number theory:

Problem 14. Let A be a finite, symmetric subset of $\mathbb{Z}^n$ containing 0. Does there exist a compact set K such that for every $x \in \mathbb{R}^n$ there exists $y \in K$ with $x \equiv y \pmod{\mathbb{Z}^n}$ and $A = (K - K) \cap \mathbb{Z}^n$?

This type of problems are one of the main topics of additive number theory. For further references see [18].

M.B. Nathanson in [19] proved that a finite, symmetric set of generators of $\mathbb{Z}$, containing 0, is of the form $(K - K) \cap \mathbb{Z}$ for some compact set $K \subset \mathbb{R}$ such that $\mathbb{R} = K + \mathbb{Z}$ by giving an explicit construction of such set K. This answers the inverse problem in the case $n = 1$.

As an attempt to attack the case $n = 2$, P. Hegarty raised the following question: Does there exist a compact set $K \subseteq \mathbb{R}^2$ such that for every $x \in \mathbb{R}^2$ there exists $y \in K$ with $x \equiv y \pmod{\mathbb{Z}^2}$ and $(K - K) \cap \mathbb{Z}^2 \subset (\mathbb{Z} \times \{0\}) \cup (\{0\} \times \mathbb{Z})$? In this paper we prove that the answer to this question is "no". This proves that the set $A = \{(-1, 0), (0, -1), (0, 0), (1, 0), (0, 1)\}$, although is a finite, symmetric set of generators of $\mathbb{Z}^2$ containing 0, is not of the form $(K - K) \cap \mathbb{Z}^2$ for any compact fundamental domain K. Thus, we obtain the negative answer to Problem 14 in the case $n = 2$ and as a corollary, the negative answer to Problem 14 in the case $n > 1$. This refines the inverse problem for $n > 1$:

Problem 15. Which sets can be obtained as $(K - K) \cap \mathbb{Z}^n$ where K is a compact set such that for every $x \in \mathbb{R}^n$ there exists $y \in K$ with $x \equiv y \pmod{\mathbb{Z}^n}$?

By using a different argument the same result was obtained by L.A. Borisov and R. Jin in [12].

2.1 The proof

We will start the proof by using the observation of R. Jin in [12]:

Theorem 16. *Let K be a compact set of $\mathbb{R}^2$. For $J = (j_1, j_2) \in \mathbb{Z}^2$, let*

$$B_{n,J} = [\frac{j_1}{n}, \frac{j_1 + 1}{n}] \times [\frac{j_2}{n}, \frac{j_2 + 1}{n}].$$

There exists an integer n_0 such that for every integer $n \geq n_0$ there is a finite

subset $\mathcal{J}$ *of* $\mathbb{Z}^2$ *such that the set*

$$K_n = \bigcup_{J \in \mathcal{J}} B_{n,J}$$

satisfies $K \subset K_n$ *and*

$$(K - K) \cap \mathbb{Z}^2 = (K_n - K_n) \cap \mathbb{Z}^2.$$

Proof. The set K is compact, thus the set $K-K$ is compact. Indeed $K-K = f(K \times K)$, where f is the continuous function $f : \mathbb{R}^2 \to \mathbb{R}$, $(x, y) \mapsto x - y$, and the image of a compact set through a continuous map is a compact set. The compactness of $K - K$ implies that there is an $\varepsilon > 0$ such that

$$\min\{|x - y| : \ x \in K - K, \ y \in \mathbb{Z}^n \setminus (K - K)\} > \varepsilon,$$

for the distance function $x \in K \mapsto d(x, \mathbb{Z}^2 \setminus (K - K)) \in \mathbb{R}$ is continuous and has a non-zero minimal value.

Let $n_0 > 4\sqrt{2}/\varepsilon$, and for $n \geq n_0$ set $\mathcal{J} = \{J \in \mathbb{Z}^2 |\ B_{n,J} \cap K \neq \emptyset\}$. It is easy to see that $(K-K)\cap\mathbb{Z}^2 \subseteq (K_n-K_n)\cap\mathbb{Z}^2$. To prove the other inclusion we will prove that $(\mathbb{Z}^2\setminus(K-K))\cap(K_n-K_n) = \emptyset$. Indeed, for any $z_1, z_2 \in K_n$ there are $x_1, x_2 \in K$ such that $|x_1 - z_1| < \sqrt{2}/n$ and $|x_2 - z_2| < \sqrt{2}/n$. We have $|(x_1 - x_2) - (z_1 - z_2)| \leq |x_1 - z_1| + |x_2 - z_2| < 2\sqrt{2}/n$. So, for any $z \in K_n - K_n$ there is an $x \in K - K$ such that $|x - z| < 2\sqrt{2}/n$. Hence, for any $y \in \mathbb{Z}^2 \setminus (K - K)$ and any $z \in K_n - K_n$,

$$|y - z| \geq |y - x| - |x - z| > \varepsilon - 2\sqrt{2}/n > \varepsilon/2 > 0.$$

□

Let K be a compact set such that $\mathbb{R}^2 = K + \mathbb{Z}^2$. In view of the previous theorem there exists $n \in \mathbb{Z}_{>0}$ such that $K \subset K_n$ and $(K - K) \cap \mathbb{Z}^2 = (K_n - K_n) \cap \mathbb{Z}^2$. So, in order to prove that $(K - K) \cap \mathbb{Z}^2$ is not contained in the coordinate axes, it suffices to prove this result for any such set K_n or any of its subsets. Thus, we reduce $\mathcal{J}$ so that $|\mathcal{J}| = n^2$ and $K_n + \mathbb{Z}^2 = \mathbb{R}^2$. We write $K_n = \bigcup_{i=0}^{n-1} \bigcup_{j=0}^{n-1} B_{i,j} + u_{i,j}$, where $B_{i,j} = [\frac{i}{n}, \frac{i+1}{n}] \times [\frac{j}{n}, \frac{j+1}{n}]$ and $u_{i,j} \in \mathbb{Z}^2$. Since the difference set $K_n - K_n$ remains invariant if we translate the set K_n by an element of $\mathbb{Z}^2$, we may assume $u_{0,0} = (0, 0)$ (see Figure 2.1).

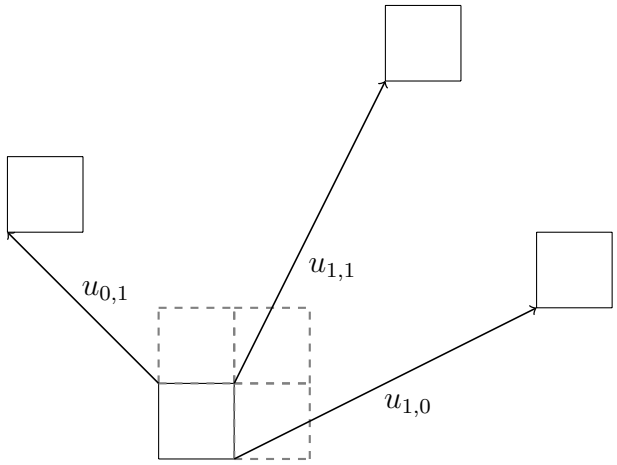

Figure 2.1: K_n with $n = 2$

Before proceeding to the proof of our main result, we will show how the set K_n defines first an element of cohomology group $H^1(T; \mathbb{Z} \times \mathbb{Z})$, and then, an isomorphism $H_1(T) \to \mathbb{Z} \times \mathbb{Z}$. We will also need two technical lemmas.

Let us consider the unit square subdivided into n^2 squares $B_{i,j}$, where $0 \leqslant i, j \leqslant n - 1$. We label the vertices $(\frac{i}{n}, \frac{j}{n})$, where $0 \leqslant i, j \leqslant n$, with the

value $v_{i,j}$ in the following way (see Figure 2.2):

$$v_{i,j} = \begin{cases} u_{i,j} & \text{for } 0 \leqslant i,j \leqslant n-1 \\ u_{0,j} + (-1,0) & \text{for } i = n, 0 \leqslant j \leqslant n-1 \\ u_{i,0} + (0,-1) & \text{for } 0 \leqslant i \leqslant n-1, j = n \\ (-1,-1) & \text{for } i = n, j = n \end{cases}$$

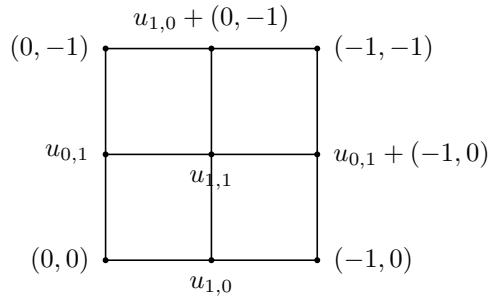

Figure 2.2: Vertices labeling

We direct the edges, the sides of the $B_{i,j}$'s, in upward and rightward direction and we label them with the value of the differences: value at the ending vertex minus value at the initial vertex (see Figure 2.3). Note that the unit square subdivided in this fashion, and with the prescribed orientation on the edges, after identifying two by two the opposite surrounding edges can be seen as the torus T with $\square$-complex structure.

If we denote the labeling of the edges by ψ, then

$$\psi([(\frac{i}{n}, \frac{j}{n}), (\frac{i+1}{n}, \frac{j}{n})]) = v_{i+1,j} - v_{i,j}, \text{ for } 0 \leqslant i \leqslant n-1, 0 \leqslant j \leqslant n$$

and

$$\psi([(\frac{i}{n}, \frac{j}{n}), (\frac{i}{n}, \frac{j+1}{n})]) = v_{i,j+1} - v_{i,j}, \text{ for } 0 \leqslant i \leqslant n, 0 \leqslant j \leqslant n-1.$$

Note that $\psi([(\frac{i}{n},0),(\frac{i+1}{n},0)]) = \psi([(\frac{i}{n},1),(\frac{i+1}{n},1)])$, for $0 \leqslant i \leqslant n-1$ and $\psi([(0,\frac{j}{n}),(0,\frac{j+1}{n})]) = \psi([(1,\frac{j}{n}),(1,\frac{j+1}{n})])$, for $0 \leqslant j \leqslant n-1$, so ψ is a well-defined function from the edges of T to the abelian group $\mathbb{Z} \times \mathbb{Z}$. Moreover, $\psi([(\frac{i}{n},\frac{j}{n}),(\frac{i+1}{n},\frac{j}{n})]) + \psi([(\frac{i+1}{n},\frac{j}{n}),(\frac{i+1}{n},\frac{j+1}{n})]) - \psi([(\frac{i}{n},\frac{j+1}{n}),(\frac{i+1}{n},\frac{j+1}{n})]) - \psi([(\frac{i}{n},\frac{j}{n}),(\frac{i}{n},\frac{j+1}{n})]) = 0$, for $0 \leqslant i,j \leqslant n-1$, so we can see ψ as one representative of an element of the cohomology group $H^1(T;\mathbb{Z}\times\mathbb{Z})$.

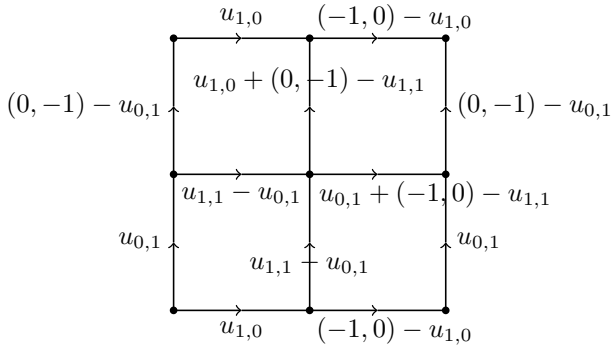

Figure 2.3: Edges labeling

There is a natural map $H^1(T;\mathbb{Z}\times\mathbb{Z}) \to \mathrm{Hom}(H_1(T),\mathbb{Z}\times\mathbb{Z})$ that sends ψ to $\overline{\psi_0} : H_1(T) \to \mathbb{Z}\times\mathbb{Z}$ where

$$\overline{\psi_0}([[(0,0),(1,0)]]) = (-1,0) \text{ and } \overline{\psi_0}([[(0,0),(0,1)]]) = (0,-1).$$

Since $H_1(T) = \mathbb{Z}\times\mathbb{Z}$ with generators $[[(0,0),(1,0)]]$ and $[[(0,0),(0,1)]]$, we obtain that $\overline{\psi_0}$ is an isomorphism. This means that

(∗) we can read the homotopy type of a closed curve from the sum of the values associated by ψ to the edges forming the curve.

Remark 17. All the values that ψ associates to the edges are in the set $K_n - K_n$. Moreover, any sum of the values of consecutive edges of a $B_{i,j}$ belongs to $K_n - K_n$.

Indeed, if one considers the vertex $(\frac{i}{n}, \frac{j}{n})$ with $0 < i, j < n$, we have $(\frac{i}{n}, \frac{j}{n}) + u_{i-1,j}$, $(\frac{i}{n}, \frac{j}{n}) + u_{i,j-1}$, $(\frac{i}{n}, \frac{j}{n}) + u_{i-1,j-1}$ and $(\frac{i}{n}, \frac{j}{n}) + u_{i,j}$ in K_n, hence

$$\left(\frac{i}{n}, \frac{j}{n}\right) + u_{i,j} - \left(\frac{i}{n}, \frac{j}{n}\right) - u_{i-1,j} = v_{i,j} - v_{i-1,j} = \psi\left(\left[\left(\frac{i-1}{n}, \frac{j}{n}\right), \left(\frac{i}{n}, \frac{j}{n}\right)\right]\right)$$

and

$$\left(\frac{i}{n}, \frac{j}{n}\right) + u_{i,j} - \left(\frac{i}{n}, \frac{j}{n}\right) - u_{i,j-1} = v_{i,j} - v_{i,j-1} = \psi\left(\left[\left(\frac{i}{n}, \frac{j-1}{n}\right), \left(\frac{i}{n}, \frac{j}{n}\right)\right]\right).$$

A similar argument holds for the edges when either i or j is equal to 0 or n.

Since the sum of the values of all consecutive edges of a $B_{i,j}$ equals 0, it suffices to prove the statement for two consecutive edges. If $0 < i, j < n$, then

$$\psi\left(\left[\left(\frac{i-1}{n}, \frac{j-1}{n}\right), \left(\frac{i}{n}, \frac{j-1}{n}\right)\right]\right) + \psi\left(\left[\left(\frac{i}{n}, \frac{j-1}{n}\right), \left(\frac{i}{n}, \frac{j}{n}\right)\right]\right) = \left(\frac{i}{n}, \frac{j}{n}\right) + u_{i,j} - \left(\frac{i}{n}, \frac{j}{n}\right) - u_{i-1,j-1}.$$

Hence the sum of the values of two consecutive edges of $B_{i,j}$, where $0 < i, j < n$ is in $K_n - K_n$. Similarly, the same holds for $B_{i,j}$ when either i or j is equal to 0 or n.

Definition 18. A component is a union of squares $B_{i,j}$, connected on the torus T.

Note that the boundary of a component is a union of simple closed curves. Indeed, let C be a component and let us denote by $\sigma = \partial C$ the boundary of C. Then σ is the union of the curves enclosing C. To prove that σ is a union of closed curves, we proceed by induction on the number m of squares in C. If $m = 1$, the component is made of just one square, so σ is the simple closed curve enclosing this square. Let $m \geq 2$, and suppose that any component having less than m squares is enclosed by a union of closed curves. Let C_0 be a square in C and let C_1 be the union of the squares in C different than C_0. Then $C = C_0 \cup C_1$. Moreover, C_1 can be seen as a disjoint union of components, each of them having less than m squares, hence enclosed by a union of closed curves. Thus, ∂C_1 is the union of closed curves. There are five possibilities for the intersection $C_0 \cap C_1$: it can be a vertex of C_0, a side of C_0 or a union of two, three or four sides of C_0. In each of the cases, we obtain that σ is the union of closed curves. As any closed curve can be seen as a union of simple closed curves, we conclude that σ is a union of simple closed curves.

Definition 19. Let C be a component. If all the simple closed curves forming the boundary of C have homotopy type 0 (i.e. are contractible on the torus T), we say that C is improper.

Lemma 20. *Let C be an improper component, and $i : C \to T$ be the inclusion map. Assume that the boundary of C is a single simple closed*

curve. Then

$$i_*(\Pi_1(C)) = \begin{cases} 0 \\ \mathbb{Z}^2 \end{cases}$$

Proof. Let $f : I \to T$ be the boundary of C, where I is the unit interval $I = [0, 1]$. We denote by $p : \mathbb{R}^2 \to T = \mathbb{R}^2/\mathbb{Z}^2$ the universal cover of T. The interval I is path-connected and locally path-connected and $f_*(\pi_1(I)) = 0 \subset 0 = p_*(\pi_1(\mathbb{R}^2))$, hence for each lift $\widetilde{f(0)}$ of $f(0)$, there is a unique path $\widetilde{f} : I \to \mathbb{R}^2$ lifting f starting at $\widetilde{f(0)}$. This holds for any map $g : J \to T$, where J is an interval in $\mathbb{R}$. As p is a covering map, it is a local homeomorphism of $\mathbb{R}^2$ with T, so f being simple implies that the lifts are simple curves as well. Moreover, $[f] = 0$, so there is a homotopy $F_t : I \to T$, $0 \leq t \leq 1$, such that $F_0 = f$ and $F_1 = f(0)$. By the homotopy lifting property, for each lift $\widetilde{f}$, there exists a unique homotopy $\widetilde{F}_t : I \to \mathbb{R}^2$ of $\widetilde{f}$ to $\widetilde{f(0)}$ that lifts F_t. Thus, $[\widetilde{f}] = 0$ and $\widetilde{f}$ is a loop. Hence, every lift $\widetilde{f}$ of f is a simple closed curve, so by Jordan curve theorem it separates $\mathbb{R}^2$ into two open, path-connected components, of which the image of $\widetilde{f}$ is the common boundary.

We fix a lift $\widetilde{f(0)}$ and consider the lifting $\widetilde{f} : I \to \mathbb{R}^2$ of f starting at $\widetilde{f(0)}$. Let us denote by $\widetilde{U}$ the interior region defined by $\widetilde{f}$ and by $\widetilde{D} = \overline{\widetilde{U}} = \widetilde{U} \cup \mathrm{Im}(\widetilde{f})$ the closure. We will prove that $p|_{\widetilde{D}}$ is injective. Let us assume the contrary, so there exist $x, y \in \widetilde{D}$ such that $x \neq y$ and $p(x) = p(y)$. Hence, there exists $a \in \mathbb{Z}^2_{\neq(0,0)}$ such that $y = x + a$. On the other hand, $\widetilde{D}$ is the closure of a connected set, so it is connected and since it is locally path-connected, $\widetilde{D}$ is path-connected. Thus there exists a path $\widetilde{\gamma} : I \to \widetilde{D}$ with $\widetilde{\gamma}(0) = x$ and

$\widetilde{\gamma}(1) = \widetilde{f(0)}$. We denote by $\widetilde{\delta}$ the closed curve

$$\widetilde{\delta}(t) = \begin{cases} \widetilde{\gamma}(t+1) & \text{for } -1 \leqslant t \leqslant 0 \\ \widetilde{f}(t) & \text{for } 0 \leqslant t \leqslant 1 \\ \widetilde{\gamma}(2-t) & \text{for } 1 \leqslant t \leqslant 2 \end{cases}$$

We have $\widetilde{\delta} : [-1, 2] \to \mathbb{R}^2$ and $\widetilde{\delta}(-1) = \widetilde{\delta}(2) = x$. Then $\delta = p\widetilde{\delta} : [-1, 2] \to T$ is the loop with $\delta(-1) = \delta(2) = p(x)$. By assumption, x and y are two different lifts of $p(x)$, so we can consider the lift $\widetilde{\delta}$ of δ starting at x and the lift $\widetilde{\delta'}$ of δ starting at y. We consider the closed curve $\widetilde{\delta} + a : I \to \mathbb{R}^2$. We have $p(\widetilde{\delta} + a) = \delta$ and $(\widetilde{\delta} + a)(-1) = y$, so by the unique lifting property $\widetilde{\delta'} = \widetilde{\delta} + a$. Now, every lift of δ contains a lift of f, since $\delta(t) = f(t)$, for $0 \leq t \leq 1$. Whence $\widetilde{f}(t) = \widetilde{\delta}(t)$, for $0 \leq t \leq 1$ is the lift of f starting at $\widetilde{f}(0)$ and $\widetilde{f'}(t) = \widetilde{\delta'}(t)$, for $0 \leq t \leq 1$ is the lift of f starting at $\widetilde{f'}(0) = \widetilde{f}(0) + a$. Furthermore, $\widetilde{f'} = \widetilde{f} + a$. Thus $\mathrm{Im}(\widetilde{f}) \cap \mathrm{Im}(\widetilde{f'}) = \emptyset$. For if $\widetilde{f}(t_1) = \widetilde{f'}(t_2)$, for some $0 \leq t_1, t_2 \leq 1$, then $\widetilde{f}(t_1) = \widetilde{f}(t_2) + a$, hence $t_1 \neq t_2$. Moreover, $f(t_1) = f(t_2)$, and since f is a simple closed curve, we obtain $t_1 = 0, t_2 = 1$ or $t_1 = 1, t_2 = 0$, a contradiction, for $\widetilde{f}(0) = \widetilde{f}(1) = x \neq y = \widetilde{f'}(0) = \widetilde{f'}(1)$. We obtained that the images of the liftings $\widetilde{f}$ and $\widetilde{f'} = \widetilde{f} + a$ of f are disjoint. We consider the intersection $\widetilde{D} \cap \widetilde{D'}$, where $\widetilde{D'}$ is the closure of the interior region defined by $\widetilde{f'}$. We have $\widetilde{D'} = \widetilde{D} + a$, so $\mu(\widetilde{D'}) = \mu(\widetilde{D})$, where by μ we denote the Lebesgue measure. Since $\mathrm{Im}(\widetilde{f})$ and $\mathrm{Im}(\widetilde{f'})$ are disjoint, we have $\mathrm{Im}(\widetilde{f}) \subset \widetilde{U'}$ or $\mathrm{Im}(\widetilde{f}) \subset (\widetilde{D'})^C$. If $\mathrm{Im}(\widetilde{f}) \subset \widetilde{U'}$, then $\widetilde{D} \subset \widetilde{U'} \subset \widetilde{D'}$ and $\mu(\widetilde{D'} \setminus \widetilde{D}) = \mu(\widetilde{D}) - \mu(\widetilde{D'}) = 0$. Having that $U' \setminus D \subset D' \setminus D$, we obtain $\mu(U' \setminus D) = 0$. This is a contradiction, for $U' \setminus D$ is open in $\mathbb{R}^2$, whence

$\mu(U' \setminus D) > 0$. We obtain $\mathrm{Im}(\widetilde{f}) \subset (\widetilde{D'})^C$. Similarly, $\mathrm{Im}(\widetilde{f'}) \subset (\widetilde{D})^C$. Hence, $\widetilde{D} \cap \widetilde{D'} = \emptyset$. On the other hand, by assumption, $y \in \widetilde{D}$ and $y = x + a \in \widetilde{D} + a = \widetilde{D'}$. This is a contradiction, so $p|_{\widetilde{D}}$ is injective.

Next, we need to prove that if $D = p(\widetilde{D})$, then $C = D$ or $C = \overline{D^C}$. First, we prove that $\mathrm{Int}(C) = C \setminus \mathrm{Im}(f)$ and $\mathrm{Int}(\overline{C^C}) = \overline{C^C} \setminus \mathrm{Im}(f) = C^C$ are connected sets in T. This is to say that f divides T into two connected components: $T \setminus \mathrm{Im}(f) = \mathrm{Int}(C) \cup \mathrm{Int}(\overline{C^C})$. As this components are open in $\mathbb{R}^2$, they are locally path-connected, and thus path-connected.

We consider $C \setminus \mathrm{Im}(f)$. The proof is by induction on the number m of squares in C. If $m = 1$, the component C is a square and the square without its border is connected. Let $m \geq 2$, and suppose that the statement is true if C consists of less than m squares. Let C_0 be a square in C touching the boundary $\mathrm{Im}(f)$ such that $C \setminus C_0$ is connected and let C_1 be the union of squares in C different than C_0. Since f is a simple closed curve, the intersection $C_0 \cap C_1$ can be one, two or three sides of C_0. In all three cases, the boundary ∂C_1 will be still a closed simple curve. Thus, by induction hypothesis, $C_1 \setminus \partial C_1$ is connected. Since the intersection $C_0 \cap C_1$ is not contained in $\mathrm{Im}(f)$, we obtain that $C \setminus \mathrm{Im}(f) = (C_0 \cup C_1) \setminus \mathrm{Im}(f)$ is connected. A similar argument holds for C^C.

Now, $p|_{\widetilde{D}}$ is injective, so $p(\widetilde{U}) \cap p(\mathrm{Im}(\widetilde{f})) = p(\widetilde{U}) \cap \mathrm{Im}(f) = \emptyset$, since $\widetilde{U} = \mathrm{Int}(\widetilde{D})$. We have $p(\widetilde{U}) \subset T \setminus \mathrm{Im}(f)$. On the other hand, the interior $\widetilde{U}$ is connected. The covering map p is continuous, whence $p(\widetilde{U})$ is connected. We obtain that $p(\widetilde{U}) \subset \mathrm{Int}(C)$ or $p(\widetilde{U}) \subset \mathrm{Int}(\overline{C^C})$, or equivalently $D = p(\widetilde{D}) \subset C$ or $D = p(\widetilde{D}) \subset \overline{C^C}$.

Let us prove that $D = C$ or $D = \overline{C^C}$, the latter being equivalent to $C = \overline{D^C}$. Let us assume that $D \subset C$. This means that $p(\widetilde{U}) \subset \mathrm{Int}(C)$. Fix $x \in p(\widetilde{U})$. There exists $\widetilde{x} \in \widetilde{U}$ such that $x = p(\widetilde{x})$. Let $y \in \mathrm{Int}(C)$. Since $\mathrm{Int}(C)$ is path-connected, there exists a path $g : I \to \mathrm{Int}(C) \subset T$ such that $g(0) = x$ and $g(1) = y$. Let $\widetilde{g} : I \to \mathbb{R}^2$ be the unique path lifting g starting at $\widetilde{x} = \widetilde{g(0)}$. Then $\widetilde{y} = \widetilde{g(1)}$ is a lift of y, i.e. $p(\widetilde{y}) = y$. Moreover, $\mathrm{Im}(\widetilde{g}) \cap \mathrm{Im}(\widetilde{f}) = \emptyset$. For, if $\widetilde{z} \in \mathrm{Im}(\widetilde{g}) \cap \mathrm{Im}(\widetilde{f})$, then $p(\widetilde{z}) \in \mathrm{Im}(g) \cap \mathrm{Im}(f)$, a contradiction, since $\mathrm{Im}(g) \subset \mathrm{Int}(C)$ and $\mathrm{Int}(C) \cap \mathrm{Im}(f) = \emptyset$. We obtain that $\mathrm{Im}(\widetilde{g}) \subset \widetilde{U}$, so $\widetilde{y} \in \widetilde{U}$ and $y \in p(\widetilde{U})$. Whence, $p(\widetilde{U}) \subset \mathrm{Int}(C)$ and $D = C$. Similarly, we conclude that if $p(\widetilde{U}) \subset \mathrm{Int}(\overline{C^C})$, then $C = \overline{D^C}$.

We are now in position of proving the statement. Let $h : I \to T$ be a closed curve in D. Then there is a unique lift $\widetilde{h} : I \to \mathbb{R}^2$ of h such that $\widetilde{h}(0) \in \widetilde{D}$. Moreover, since $p|_{\widetilde{D}}$ is injective and $h(0) = h(1)$, we have $\widetilde{h}(0) = \widetilde{h}(1)$, so $\widetilde{h}$ is a closed curve in $\mathbb{R}^2$, hence $[\widetilde{h}] = 0$. Having that $h = p(\widetilde{h})$, we obtain $[h] = [p \circ \widetilde{h}] = p_*(\widetilde{h}) = 0$. This means that if $j : D \to T$ denotes the inclusion map, then $j_*(\pi_1(D)) = 0$. But, we already proved that $C = D$ or $C = \overline{D^C}$. Thus, if $C = D$, then $i_*(\pi_1(C)) = 0$. On the other hand, if $C = \overline{D^C}$, then as $j_*(\pi_1(D)) = 0$, Van Kampen's theorem implies $i_*(\pi_1(C)) = \mathbb{Z}^2$.

□

Corollary 21. *Let C be an improper component. Then*

$$i_*(\pi_1(C)) = \begin{cases} 0 \\ \mathbb{Z}^2 \end{cases}$$

Proof. First, we consider the case when the $\mathrm{Int}(C)$ is connected. In this case,

as $\mathrm{Int}(C)$ is locally path-connected, whence $\mathrm{Int}(C)$ is path-connected. The boundary of C is a union of simple closed curves which are contractible on the torus. Let $f : I \to T$ be a simple closed curve that is a part of the boundary of C. Arguing as in the previous lemma, every lift $\widetilde{f}$ of f is a simple closed curve and, by Jordan curve theorem, it separates $\mathbb{R}^2$ into two open, path-connected components, of which the image of $\widetilde{f}$ is the common boundary. Let us fix a lift $\widetilde{f}$ of f and let $\widetilde{U}$ be the interior region defined by $\widetilde{f}$. By the previous lemma, $p|_{\widetilde{D}}$ is injective, where $\widetilde{D} = \overline{\widetilde{U}}$. Two possibilities may occur: $p(\widetilde{U}) \cap \mathrm{Int}(C) \neq \emptyset$ or $p(\widetilde{U}) \cap \mathrm{Int}(C) = \emptyset$. Let us consider the case $p(\widetilde{U}) \cap \mathrm{Int}(C) \neq \emptyset$. As $\mathrm{Int}(C)$ is path-connected, we obtain $\mathrm{Int}(C) \subset p(\widetilde{U})$. Thus, we have $\mathrm{Int}(C) \subset p(\widetilde{U})$ or $p(\widetilde{U}) \cap \mathrm{Int}(C) = \emptyset$, the latter being equivalent to $p(\widetilde{U}) \subset C^C$. If $\mathrm{Int}(C) \subset p(\widetilde{U})$, then $\mathrm{Int}(C) \subset (\bigcup_{a\in\mathbb{Z}^2} p(\widetilde{U} + a)) = p(\bigcup_{a\in\mathbb{Z}^2}(\widetilde{U} + a))$, where $\widetilde{U} + a$, when a ranges through $\mathbb{Z}^2$, represents the interior regions of all liftings of f. Hence, $p^{-1}(\mathrm{Int}(C)) \subset \bigcup_{a\in\mathbb{Z}^2}(\widetilde{U} + a)$. On the other hand, if $p(\widetilde{U}) \cap \mathrm{Int}(C) = \emptyset$, then $p(\bigcup_{a\in\mathbb{Z}^2}(\widetilde{U} + a)) \cap \mathrm{Int}(C) = \emptyset$, so $p^{-1}(\mathrm{Int}(C)) \subset (\bigcup_{a\in\mathbb{Z}^2}(\widetilde{U} + a))^C = \bigcap_{a\in\mathbb{Z}^2}(\widetilde{U} + a)^C$. We conclude that $p^{-1}(C) \subset \bigcup_{a\in\mathbb{Z}^2}(\widetilde{D} + a)$ or $p^{-1}(C) \subset \bigcap_{a\in\mathbb{Z}^2}(\widetilde{U} + a)^C$.

Now, each of the simple closed curves making the boundary of C is lifted to simple closed curves through p and each lift defines an interior and an exterior region. Let D be the union of the closures of the interior regions and E be the intersection of the closures of the exterior regions. By the previous argument, we obtain that $p^{-1}(C) \subset D$ or $p^{-1}(C) \subset E$, and since p is surjective, we have $C \subset p(D)$ or $C \subset p(E)$.

If $C \subset p(E)$, we actually have the equality $C = p(E)$. Indeed, if $p(E) \setminus$

$C \neq \emptyset$, then exists a square S in $p(E)$ not belonging to C such that $S \cap C \neq \emptyset$. For, if that is not the case, $p(E) = (\bigcup_{S \in p(E)} S) \cup C$ would be a disconnection, which would contradict the fact that $p(E)$ is connected. But this would mean that there exists $x \in S$ such that $p^{-1}(x) \subset \bigcup_{a \in \mathbb{Z}^2} (\widetilde{U} + a)$, where $\widetilde{U}$ is an interior region of a lifting of one of the simple closed curves making the border of C. A contradiction, since there exists $y \in p^{-1}(x)$ such that $y \in E$ and $E \cap \bigcup_{a \in \mathbb{Z}^2} (\widetilde{U} + a) = \emptyset$.

On the other hand, by the previous lemma and Van Kampen's theorem, we have $j_*(\pi_1(p(D))) = 0$, where $j : p(D) \to T$ is the inclusion map. Having that $D \cup E = \mathbb{R}^2$, we obtain that $p(D) \cup p(E) = T$ and, by Van Kampen's theorem, $k_*(\pi_1(p(E))) = \mathbb{Z} \times \mathbb{Z}$, where $k : p(E) \to T$ is the inclusion map. By the previous discussion, $C \subset p(D)$ or $C = p(E)$, which ends the proof in the case when $\mathrm{Int}(C)$ is connected.

Finally, let us define the wedge sum as a union of two sets intersecting at only one point. Then any improper component C can be seen as the wedge sum of improper components with connected interiors. The statement follows by Van Kampen's theorem.

□

Theorem 22. *There does not exist a compact set K such that $\mathbb{R}^2 = K + \mathbb{Z}^2$ and $(K - K) \cap \mathbb{Z}^2 \subseteq (\mathbb{Z} \times \{0\}) \cup (\{0\} \times \mathbb{Z})$.*

Proof. We prove by contradiction. Let us assume that such set K exists. Then, there exists $n \in \mathbb{Z}_{>0}$ such that $(K_n - K_n) \cap \mathbb{Z}^2 \subseteq (\mathbb{Z} \times \{0\}) \cup (\{0\} \times \mathbb{Z})$, where $K_n = \bigcup_{i=0}^{n-1} \bigcup_{j=0}^{n-1} B_{i,j} + u_{i,j}$, with $B_{i,j} = [\frac{i}{n}, \frac{i+1}{n}] \times [\frac{j}{n}, \frac{j+1}{n}]$ and $u_{i,j} \in \mathbb{Z}^2$.

We will prove that this is absurd.

By Remark 17, we have that the values that ψ associates to the edges are either in the x-axis, the y-axis or equal to $(0,0)$. Therefore, we can color the edges in the following way: red if the value of the edge lays on the x-axis and it is different than $(0,0)$, blue if the value of the edge lays on the y-axis and it is different than $(0,0)$, and white if the value of the edge is $(0,0)$. Moreover, since any sum of the values of consecutive edges of a $B_{i,j}$ belongs to $K_n - K_n$, the square cannot have a red and a blue edge at the same time. We obtain that all the squares can have only red and white edges, blue and white edges, or all white edges. We will be calling them red, blue and white squares, respectively. Note that the common edge between a red and a blue square is white.

Let C be a monochromatic collection of squares, maximal with respect to inclusion, such that when seen on the surface of the torus it is connected. We now prove that C is an improper component.

Given a curve, we call *gain* the sum of the values associated by ψ to the edges forming it. A gain of value $(\cdot, 0)$ can only be obtained through red squares; a gain of value $(0, \cdot)$ can only be obtained through blue squares. Therefore, because the gain of the horizontal curve $[[(0,0),(1,0)]]$ is $(-1,0)$ and the gain of the vertical curve $[[(0,0),(0,1)]]$ is $(0,-1)$, the coloring must contain red, as well as blue component. Thus, the boundary of a component is a union of simple closed curves formed by white edges only. Hence, by $(*)$, the boundary of a component is a union of simple closed curves which are contractible on the torus. We conclude that C is an improper component.

We will reach a contradiction using the corollary above. Let us consider any red component. If the component is contractible on the torus any horizontal line that crosses the component will have a horizontal gain equal to $(0, 0)$ inside the component. The horizontal gain $(-1, 0)$ is obtained only through red squares, so there exists a red component that is non-contractible on the torus. On the other hand, it follows from Corollary 21, that if a component has a boundary that consists of simple closed curves which are contractible on the torus, then it is either contractible on the torus or it contains loops generating the fundamental group of the torus. Whence, there exists a red component inside of which we can obtain both gains, $(-1, 0)$ and $(0, -1)$. A contradiction.

□

Corollary 23. *Let $n \in \mathbb{Z}_{>1}$. For $1 \leq i \leq n$, let $e_i \in \mathbb{R}^n$ be the vector with 1 in the ith position and 0's in all other positions. The set $A = \{(0, \ldots, 0)\} \cup \{\pm e_i \mid 1 \leq i \leq n\}$ is a finite, symmetric subset of $\mathbb{Z}^n$ containing 0. Then A is not of the form $(K - K) \cap \mathbb{Z}^n$ for any compact set K such that for every $x \in \mathbb{R}^n$ there exists $y \in K$ with $x \equiv y \pmod{\mathbb{Z}^n}$.*

Proof. Assume on the contrary that $A = (K - K) \cap \mathbb{Z}^n$ for some compact set K such that for every $x \in \mathbb{R}^n$ there exists $y \in K$ with $x \equiv y \pmod{\mathbb{Z}^n}$. Let $p : \mathbb{R}^n \to \mathbb{R}e_1 + \mathbb{R}e_2$ be the orthogonal projection. We will identify $\mathbb{R}^2$ with $\mathbb{R}e_1 + \mathbb{R}e_2$ and $\mathbb{Z}^2$ with $\mathbb{Z}e_1 + \mathbb{Z}e_2$. Then

$$p(A) = \{(-1, 0), (0, -1), (0, 0), (1, 0), (0, 1)\} = (p(K) - p(K)) \cap \mathbb{Z}^2,$$

where $p(K) \subset \mathbb{R}^2$ is a compact set such that for every $x \in \mathbb{R}^2$ there exists $y \in p(K)$ with $x \equiv y \pmod{\mathbb{Z}^2}$, a contradiction.

□

Chapter 3

On a partition problem of Canfield and Wilf

The content of this chapter is a joint work with M. B. Nathanson, [14].

Let A be a nonempty set of positive integers. A *partition of n with parts in A* is a representation of n in the form

$$n = \sum_{a \in A} m_a a$$

where $m_a \in \mathbf{N} \cup \{0\}$ for all $a \in A$, and $m_a \in \mathbf{N}$ for only finitely many a. Let $p_A(n)$ denote the number of partitions of n with parts in A. If $\gcd(A) = d > 1$, then $p_A(n) = 0$ for all n not divisible by d, ands so $p_A(n) = 0$ for infinitely many positive integers n. If $p_A(n) \geq 1$ for all sufficiently large n, then $\gcd(A) = 1$.

If $A = \{a_1, \ldots, a_k\}$ is a set of k relatively prime positive integers, then Schur [27] proved that

$$p_A(n) \sim \frac{n^{k-1}}{(k-1)!a_1a_2\cdots a_k}. \tag{3.1}$$

Nathanson [23] gave a simpler proof of the more precise result:

$$p_A(n) = \frac{n^{k-1}}{(k-1)!a_1a_2\cdots a_k} + O\left(n^{k-2}\right). \tag{3.2}$$

An arithmetic function is a real-valued function whose domain is the set $\mathbf{N}$ of positive integers. An arithmetic function f has *polynomial growth* if there is a positive integer k and an integer $N_0(k)$ such that $f(n) \leq n^k$ for all $n \geq N_0(k)$. Equivalently, f has polynomial growth if

$$\limsup_{n\to\infty} \frac{\log f(n)}{\log n} < \infty.$$

An arithmetic function f has *superpolynomial growth* if

$$\lim_{n\to\infty} \frac{\log f(n)}{\log n} = \infty.$$

The asymptotic formula (3.1) implies the following result of Nathanson [21, Theorem 15.2, pp. 458–461].

Theorem 24. *If A is an infinite set of integers and $\gcd(A) = 1$, then $p_A(n)$ has superpolynomial growth.*

Canfield and Wilf [4] studied the following variation of the classical partition problem. Let A and M be nonempty sets of positive integers. A *partition of n with parts in A and multiplicities in M* is a representation of n in the

form

$$n = \sum_{a \in A} m_a a$$

where $m_a \in M \cup \{0\}$ for all $a \in A$, and $m_a \in M$ for only finitely many a. We denote by $p_{A,M}(n)$ the number of partitions of n with parts in A and multiplicities in M. Note that $p_{A,M}(0) = 1$ and $p_{A,M}(n) = 0$ for all $n < 0$.

Let A and M be infinite sets of positive integers such that $p_{A,M}(n) \geq 1$ for all sufficiently large n. Canfield and Wilf ("Unsolved problem 1" in [4]) asked, "Must $p_{A,M}(N)$ then be of superpolynomial growth?" We prove that the answer is "no."

3.1 Weakly superpolynomial functions

Polynomial and superpolynomial growth functions were first studied in connection with the growth of finitely and infinitely generated groups (cf. Grigorchuk and Pak [9], Nathanson [24]). Growth functions of groups are always strictly increasing, but even strictly increasing functions that do not have polynomial growth are not necessarily superpolynomial.

We shall call an arithmetic function *weakly superpolynomial* if it does not have polynomial growth. Equivalently, the function f is weakly superpolynomial if for every positive integer k there are infinitely many positive integers n such that $f(n) > n^k$. The partition functions that will be constructed in this paper are weakly superpolynomial but not superpolynomial.

We note that an arithmetic function f is weakly superpolynomial but not

superpolynomial if and only if

$$\limsup_{n\to\infty} \frac{\log f(n)}{\log n} = \infty$$

and

$$\liminf_{n\to\infty} \frac{\log f(n)}{\log n} < \infty.$$

In this section we construct a strictly increasing arithmetic function that is weakly superpolynomial but not polynomial.

Let $(n_k)_{k=1}^{\infty}$ be a sequence of positive integers such that $n_1 = 1$ and

$$n_{k+1} > 2n_k^k$$

for all $k \geq 1$. We define the arithmetic function

$$f(n) = n_k^k + (n - n_k) \qquad \text{for } n_k \leq n < n_{k+1}.$$

This function is strictly increasing because

$$n_k^k - n_k \leq n_{k+1}^{k+1} - n_{k+1}$$

for all $k \geq 1$. We have

$$\lim_{k\to\infty} \frac{\log f(n_k)}{\log n_k} = \lim_{k\to\infty} \frac{k \log n_k}{\log n_k} = \infty$$

and so

$$\limsup_{n\to\infty} \frac{\log f(n)}{\log n} = \infty.$$

Therefore, the function f does not have polynomial growth.

For every positive integer n there is a positive integer k such that $n_k \leq n < n_{k+1}$. Then $f(n) = n + n_k^k - n_k \geq n$ and so

$$\liminf_{n\to\infty} \frac{\log f(n)}{\log n} \geq 1. \tag{3.3}$$

The inequalities

$$f(n_{k+1}-1) = n_k^k + (n_{k+1}-1-n_k) < \frac{3n_{k+1}}{2}$$

and

$$n_{k+1} - 1 > \frac{n_{k+1}}{2}$$

imply that

$$1 < \frac{\log f(n_{k+1}-1)}{\log(n_{k+1}-1)} < \frac{\log(3n_{k+1}/2)}{\log(n_{k+1}/2)} = 1 + \frac{\log 3}{\log(n_{k+1}/2)}$$

and so

$$\lim_{k\to\infty} \frac{\log f(n_{k+1}-1)}{\log(n_{k+1}-1)} = 1.$$

Therefore,

$$\liminf_{n\to\infty} \frac{\log f(n)}{\log n} \leq 1. \tag{3.4}$$

Combining (3.3) and (3.4), we obtain

$$\liminf_{n\to\infty} \frac{\log f(n)}{\log n} = 1.$$

Thus, the function f has weakly superpolynomial but not superpolynomial growth.

3.2 Weakly superpolynomial partition functions

Theorem 25. *Let a be an integer, $a \geq 2$, and let $A = \{a^i\}_{i=0}^{\infty}$. Let M be an infinite set of positive integers such that M contains $\{1, 2, \ldots, a-1\}$*

and no element of M is divisible by a. Then $p_{A,M}(n) \geq 1$ for all $n \in \mathbf{N}$, and $p_{A,M}(n) = 1$ for all $n \in A$. In particular, the partition function $p_{A,M}$ does not have superpolynomial growth.

Proof. Every positive integer n has a unique a-adic representation, and so $p_{A,M}(n) \geq 1$ for all $n \in \mathbf{N}$.

We shall prove that the only partition of a^r with parts in A and multiplicities in M is $a^r = 1 \cdot a^r$. If there were another representation, then it could be written in the form

$$a^r = \sum_{i=1}^{k} m_i a^{j_i}$$

where $k \geq 2$, $m_i \in M$ for $i = 1, \ldots, k$, and $0 \leq j_1 < j_2 < \cdots < j_k < r$. Then

$$a^{r-j_1} = m_1 + a \sum_{i=2}^{k} m_i a^{j_i - j_1 - 1}.$$

We have $j_i - j_1 - 1 \geq 0$ for $i = 2, \ldots, k$, and so m_1 is divisible by a, which is absurd. Therefore, $p_{A,M}(a^r) = 1$ for all $r \geq 0$. It follows that

$$\liminf_{n \to \infty} \frac{\log p_{A,M}(n)}{\log n} = \liminf_{r \to \infty} \frac{\log p_{A,M}(a^r)}{\log a^r} = 0$$

and so the partition function $p_{A,M}$ is not superpolynomial. □

Theorem 26. *Let A and M be infinite sets of positive integers, and let $p_{A,M}(n)$ denote the number of partitions of n with parts in A and multiplicities in M. If $A(x) \geq c \log x$ for some $c > 0$ and all $x \geq x_0(A)$, then for every positive integer k there exist infinitely many integers n such that*

$$p_{A,M}(n) \geq n^k.$$

In particular, the partition function $p_{A,M}$ is weakly superpolynomial.

Proof. Let $x \geq 1$ and let

$$A(x) = \sum_{\substack{a \in A \\ a \leq x}} 1 \qquad \text{and} \qquad M(x) = \sum_{\substack{m \in M \\ m \leq x}} 1$$

denote the counting functions of the sets A and M, respectively. If $n \leq x$ and $n = \sum_{a \in A} m_a a$ is a partition of n with parts in A and multiplicities in M, then $a \leq x$ and $m_a \leq x$, and so

$$\max \{p_{A,M}(n) : n \leq x\} \leq \sum_{n \leq x} p_{A,M}(n) \leq (M(x)+1)^{A(x)}. \tag{3.5}$$

Conversely, if the integer n can be represented in the form $n = \sum_{a \in A} m_a a$ with $a \leq x$ and $m_a \leq x$, then $n \leq x^2 A(x)$ and so

$$\sum_{n \leq x^2 A(x)} p_{A,M}(n) \geq (M(x)+1)^{A(x)} > M(x)^{A(x)}.$$

Choose an integer n_x such that

$$p_{A,M}(n_x) = \max \left\{ p_{A,M}(n) : n \leq x^2 A(x) \right\}.$$

Then $n_x \leq x^3$ and

$$M(x)^{A(x)} < \sum_{n \leq x^2 A(x)} p_{A,M}(n) \leq \left(x^2 A(x) + 1 \right) p_{A,M}(n_x) \leq 2x^3 p_{A,M}(n_x)$$

and so, for all $x \geq x_0(A)$,

$$p_{A,M}(n_x) > \frac{M(x)^{A(x)}}{2x^3} \geq \frac{M(x)^{c \log x}}{2x^3}.$$

Let k be a positive integer. Because the set M is infinite, there exists $x_1(A,k) \geq x_0(A)$ such that, for all $x \geq x_1(A,k)$, we have

$$\log M(x) > \frac{2}{c \log x} + \frac{3k+3}{c}$$

and so

$$p_{A,M}(n_x) > x^{3k} \geq n_x^k.$$

We shall iterate this process to construct inductively an infinite set of integers $\{n_{x_i} : i = 1, 2, \ldots\}$ such that

$$p_{A,M}(n_{x_i}) > n_{x_i}^k$$

for all i. Let $r \geq 1$, and suppose that the integers $n_{x_1}, \ldots, n_{x_r}$ have been constructed. Choose x_{r+1} so that

$$x_{r+1}^{3k} > \left(M\left(x_i^2 A(x_i)\right) + 1\right)^{A\left(x_i^2 A(x_i)\right)}$$

for all $i = 1, \ldots, r$, and let $n_{x_{r+1}}$ be the integer constructed according to procedure above. Replacing x with $x_i^2 A(x_i)$ in inequality (3.5), we see that

$$p\left(n_{x_i}\right) \leq \left(M\left(x_i^2 A(x_i)\right) + 1\right)^{A\left(x_i^2 A(x_i)\right)}$$

and so

$$p\left(n_{x_{r+1}}\right) > x_{r+1}^{3k} > p\left(n_{x_i}\right)$$

for $i = 1, \ldots, r$, and so $n_{x_{r+1}} \neq n_{x_i}$ for $i = 1, \ldots, r$. This completes the induction and the proof. □

Theorem 27. *The partition function for the sets A and M constructed in Theorem 25 is weakly superpolynomial.*

Proof. For $a \geq 2$, the counting function for the set $A = \{a^i\}_{i=1}^{\infty}$ is $A(x) = [\log x] + 1 > \log x$, and the result follows from Theorem 26. $\square$

Chapter 4

A Lower Bound for the Size of a Sum of Dilates

Let k be an integer and let A be a finite set of integers. The k-dilation $k \cdot A$ of the set A is the set of all integers of the form ka, where $a \in A$. Let $f(x_1, \ldots, x_n) = u_1x_1 + \cdots + u_nx_n$ be a linear form with integer coefficients $u_1, \ldots, u_n$. We define the set $f(A) = u_1 \cdot A + \cdots + u_n \cdot A = \{u_1a_1 + \cdots + u_ha_n : a_i \in A\}$. B. Bukh, in [3] obtained the almost sharp lower bound for the size of the sets $f(A)$: $|u_1 \cdot A + \cdots u_n \cdot A| \geq (|u_1| + \cdots + |u_n|)|A| - o(|A|)$, where $u_1, \ldots, u_n$ are integers such that $(u_1, \ldots, u_n) = 1$.

In the case of binary linear forms we write $f(x, y) = mx + ky$, where m and k are nonzero integers. We are interested in finding a sharp lower bound for $|f(A)|$. It is easy to see ([20]) that it is enough to consider only normalized binary linear forms satisfying $k \geq |m| \geq 1$ and $(m, k) = 1$. Many authors ([3],[5],[6],[22]) studied the lower bounds of $|f(A)|$ for the case $m = 1$. The

sharp lower bound for $|A+k\cdot A|$ was known for the case $k=1$ (see [18]), and it was given for $k=2$ in [22] and $k=3$ in [6]. J. Cilleruelo, M. Silva, C. Vinuesa conjectured in [6] that if k is a positive integer and A a finite set of integers with sufficiently large cardinality, then $|A+k\cdot A| \geq (k+1)|A| - \lceil k(k+2)/4 \rceil$. This conjecture was proved for the case when k is a prime number in [5], and very recently for the cases when k is a power of a prime or a product of two primes in [7].

The case $m=2$ was studied in [10]. Y. O. Hamidoune and J. Rué proved in [10] that if k is an odd prime and A a finite set of integers such that $|A| > 8k^k$, then $|2\cdot A + k\cdot A| \geq (k+2)|A| - k^2 - k + 2$. In this paper, we extend this result to the cases when k is a prime power or a product of two primes. More precisely, we prove the following theorems.

Theorem 28. *Let A be a finite set of integers such that $|A| > 8k^k$. If $k = p^\alpha$, where p is an odd prime and $\alpha \in \mathbb{Z}_{\geq 1}$, then*

$$|2\cdot A + k\cdot A| \geq (k+2)|A| - k^2 - k + 2.$$

Theorem 29. *Let A be a finite set of integers such that $|A| > 8k^k$. If $k = pq$, where p and q are distinct odd primes, then*

$$|2\cdot A + k\cdot A| \geq (k+2)|A| - k^2 - k + 2.$$

4.1 Notation and Preliminaries

Let A be a finite set of integers and let k be a positive integer. We define $\hat{A}$ to be the natural projection of the set A on $\mathbb{Z}/k\mathbb{Z}$ and $c_k(A) = |\hat{A}|$. Then,

if $c_k(A) = j$, we denote by A_1, $A_2, \ldots, A_j$ the distinct congruence classes of A modulo k. We assume that $|A_1| \geq |A_2| \geq \ldots \geq |A_j|$. For every $1 \leq i \leq j$, we write $A_i = kX_i + u_i$, where $0 \leq u_i < k$. Let $E = \{1 \leq i \leq j \mid |\hat{X}_i| < k\}$ and let $F = \{1 \leq i \leq j \mid |\hat{X}_i| = k\}$. We define the sets $\Delta_{ii} = (2A_i + k \cdot A) \setminus (2A_i + k \cdot A_i)$ for $1 \leq i \leq j$.

Lemma 30 (Chowla, [18])**.** *Let $n \geq 2$ and let A and B be nonempty subsets of $\mathbb{Z}/n\mathbb{Z}$. If $0 \in B$ and $(b, n) = 1$ for all $b \in B \setminus \{0\}$, then*

$$|A + B| \geq \min\{n, |A| + |B| - 1\}.$$

The following proposition, as well as its corollaries and the following lemma are Proposition 3.2, Corollary 3.3, Corollary 3.4 and Lemma 4.1 from [10].

Proposition 31. *Let A and B be finite set of integers and let n and m be coprime integers. Then*

$$|n \cdot A + m \cdot B| \geq c_n(B)|A| + c_m(A)|B| - c_m(A)c_n(B).$$

Corollary 32. *Let $2 \leq n < m$ be coprime integers. Let A be a finite set of integers. Then $|n \cdot A + m \cdot A| \geq 4|A| - 4$.*

Corollary 33. *Let k be an odd integer. Let A be a finite set of integers such that $c_k(A) = k$. Then $|2 \cdot A + k \cdot A| \geq (k + 2)|A| - 2k$.*

Lemma 34. *Let A be a finite set of integers and let k be a positive integer. Then*

$$\sum_{i=1}^{j} \Delta_{ii} \geq j(j - 1).$$

In the proof of Theorem 29, we will use the following lemmas. They appear as Lemma 6 and Lemma 8 in [7].

Lemma 35. *Let k be a positive integer and let A be a nonempty subset of $\mathbb{Z}/k\mathbb{Z}$. Let α be a nonzero element in $\mathbb{Z}/k\mathbb{Z}$. We have $A + \alpha = A$ if and only if*

$$A = \bigcup_{\beta \in I} ((k, \alpha) \cdot \{0, 1, \ldots, \frac{k}{(k, \alpha)} - 1\} + \beta)$$

for some nonempty set $I \subset \mathbb{Z}/(k, \alpha)\mathbb{Z}$ and $\frac{k}{(k,\alpha)} \mid |A|$.

Lemma 36. *Let $k > 2$ be an integer that is not a prime and let A be a nonempty subset of $\mathbb{Z}/k\mathbb{Z}$. Let $(q, k) \neq 1$ and $0 \in B \subset \{0, \bar{q}\} \cup \{\bar{b} \mid (b, k) = 1\}$. If $|A + \{0, \bar{q}\}| \geq |A| + 1$, then*

$$|A + B| \geq \min(k, |A| + |B| - 1).$$

4.2 The case $k = p^\alpha$

Lemma 37. *Let A be a finite set of integers such that $\gcd(A) = 1$ and $0 \in A$. Let $k = p^\alpha$, where p is an odd prime number and $\alpha \in \mathbb{Z}_{\geq 1}$. If $|\Delta_{ii}| < |A_i|$, then $c_2(A_i) = 2$.*

Proof. Let us assume that $c_2(A_i) = 1$. Thus, A_i contains only even or only odd integers.

Let A_i contains only even integers. There exists an odd $a \in A$, since $\gcd(A) = 1$. Then

$$|\Delta_{ii}| = |(2 \cdot A_i + k \cdot A) \setminus (2 \cdot A_i + k \cdot A_i)| \geq |(2 \cdot A_i + ka)| = |A_i|,$$

a contradiction.

Similarly, if A_i contains only odd integers

$$|\Delta_{ii}| = |(2 \cdot A_i + k \cdot A) \setminus (2 \cdot A_i + k \cdot A_i)| \geq |(2 \cdot A_i + k0)| = |A_i|,$$

a contradiction. □

Lemma 38. *Let A be a finite set of integers such that $\gcd(A) = 1$. Let $k = p^\alpha$, where p is an odd prime number and $\alpha \in \mathbb{Z}_{\geq 1}$. Let $m = \min\{1 \leq i \leq j \mid p \nmid u_i\}$ and $i \in E$.*

(i) If $p \mid u_i$, then $|\Delta_{ii}| \geq |A_m|$.

(ii) If $u_l = 0$ and $p \nmid u_i$, then $|\Delta_{ii}| \geq |A_l|$.

Proof. (i) We have

$$|\Delta_{ii}| = |(2 \cdot A_i + k \cdot A) \setminus (2 \cdot A_i + k \cdot A_i)| \geq |(2 \cdot X_i + A_m) \setminus (2 \cdot X_i + A_i)|. \quad (4.1)$$

On the other hand $(u_m - u_i, k) = 1$, so using Lemma 30 and that $|X_i| < k$, we obtain

$$|2 \cdot \hat{X}_i + \{0, u_m - u_i\}| \geq |\hat{X}_i| + 1,$$

thus

$$|(2 \cdot \hat{X}_i + u_m) \setminus (2 \cdot \hat{X}_i + u_i)| \geq 1. \quad (4.2)$$

Combining (1.2) and (1.3), we conclude

$$|\Delta_{ii}| \geq |A_m||(2 \cdot \hat{X}_i + u_m) \setminus (2 \cdot \hat{X}_i + u_i)| \geq |A_m|.$$

(ii) Similarly as in (i),

$$|\Delta_{ii}| = |(2 \cdot A_i + k \cdot A) \setminus (2 \cdot A_i + k \cdot A_i)| \geq |(2 \cdot X_i + A_l) \setminus (2 \cdot X_i + A_i)|.$$

We have $(u_l - u_i, k) = 1$, so

$$|(2 \cdot \hat{X}_i + u_l) \setminus (2 \cdot \hat{X}_i + u_i)| \geq 1$$

and

$$|\Delta_{ii}| \geq |A_l||(2 \cdot \hat{X}_i + u_l) \setminus (2 \cdot \hat{X}_i + u_i)| \geq |A_l|.$$

□

Lemma 39. *Let A be a finite set of integers. If $k = p^\alpha$, where p is an odd prime and $\alpha \in \mathbb{Z}_{\geq 1}$, then*

$$|2 \cdot A + k \cdot A| \geq (k+2)|A| - 4k^{k-1}.$$

Proof. Let T be the set of integers t such that for every finite set $A \subset \mathbb{Z}$

$$|2 \cdot A + k \cdot A| \geq (t+2)|A| - 4k^{t-1}.$$

We will use induction to prove $k \in T$. By Corollary 32, we obtain that $2 \in T$. Let us assume that $2 \leq t \leq k$ and $t-1 \in T$. Let A be a finite set of integers.

Case 1. $\sum_{i \in E} |\Delta_{ii}| \geq \sum_{i \in E} |A_i|$

By Corollary 33, for every $i \in F$, we have $|2 \cdot A_i + k \cdot A_i| \geq (k+2)|A_i| - 2k$. On the other hand, if $i \in E$, using the induction hypothesis we get $|2 \cdot A_i + k \cdot A_i| \geq (t+1)|A_i| - 4k^{t-2}$. Hence,

$$
\begin{aligned}
|2\cdot A + k\cdot A| &= \sum_{i\in E}|2\cdot A_i + k\cdot A| + \sum_{i\in F}|2\cdot A_i + k\cdot A| \\
&\geq \sum_{i\in E}(|2\cdot A_i + k\cdot A| + |\Delta_{ii}|) + \sum_{i\in F}|2\cdot A_i + k\cdot A_i| \\
&\geq \sum_{i\in E}[(t+1)|A_i| - 4k^{t-2}] + \sum_{i\in E}|\Delta_{ii}| + \sum_{i\in F}[(k+2)|A_i| - 2k] \\
&\geq \sum_{i\in E}[(t+1)|A_i| - 4k^{t-2}] + \sum_{i\in E}|A_i| + \sum_{i\in F}[(k+2)|A_i| - 2k] \\
&\geq (t+2)|A| - (4|E|k^{t-2} + 2|F|k) \geq (t+2)|A| - 4k^{t-1}.
\end{aligned}
$$

Case 2. $\sum_{i\in E}|\Delta_{ii}| < \sum_{i\in E}|A_i|$.

Without loss of generality we may assume that $\gcd(A) = 1$ and $0 \in A_1$. We define $n = \min\{i \in E \mid |\Delta_{ii}| < |A_i|\}$. By Lemma 37, we have $c_2(A_n) = 2$. Let $m = \min\{1 \leq i \leq j \mid p \nmid u_i\}$. By Lemma 38, we have that $|\Delta_{ii}| \geq |A_m|$ for all $i \in E$. Note that $m \neq n$.

We have $m > n$. For if $m < n$, by Lemma 38, we have that $|\Delta_{ii}| \geq |A_n|$ for all $i \in E$ such that $i \geq n$ and this leads to contradiction:

$$
\begin{aligned}
\sum_{i\in E}|\Delta_{ii}| &= \sum_{i\in E, i<n}|\Delta_{ii}| + \sum_{i\in E, i\geq n}|\Delta_{ii}| \\
&\geq \sum_{i\in E, i<n}|A_i| + \sum_{i\in E, i\geq n}|A_n| \geq \sum_{i\in E}|A_i|.
\end{aligned}
$$

Next, by the definition of m, we have $p \mid u_n, \ldots, p \mid u_{m-1}$, so $(u_n - u_m, k) = \cdots = (u_{m-1} - u_m, k) = 1$. Using Lemma 30, we obtain

$$
|2\cdot \hat{X}_m + \{0, u_n - u_m, \ldots, u_s - u_m\}| \geq \min\{k, |\hat{X}_m| + s - n + 1\},
$$

for all $n \leq s \leq m-1$. Let $s = n$. If $|\hat{X}_m| < k$, we have

$$|(2 \cdot \hat{X}_m + u_n) \setminus (2 \cdot \hat{X}_m + u_m)| \geq 1$$

and

$$|(2 \cdot X_m + A_n) \setminus (2 \cdot X_m + A_m)| \geq |A_n|.$$

Now, let $n < s < m-1$ such that

$$|(2 \cdot X_m + (A_n \cup A_{n+1} \cup \ldots \cup A_s)) \setminus (2 \cdot X_m + A_m)| \geq |A_n| + |A_{n+1}| + \cdots + |A_s|$$

and let us assume that $|\hat{X}_m| + s - n + 2 \leq k$. We have

$$|(2 \cdot \hat{X}_m + \{u_n, \ldots, u_s\}) \setminus (2 \cdot \hat{X}_m + u_m)| \geq s - n + 1$$

and

$$|(2 \cdot \hat{X}_m + \{u_n, \ldots, u_s, u_{s+1}\}) \setminus (2 \cdot \hat{X}_m + u_m)| \geq s - n + 2,$$

so

$$|(2 \cdot X_m + (A_n \cup A_{n+1} \cup \ldots \cup A_{s+1}) \setminus (2 \cdot X_m + A_m)| \geq |A_n| + |A_{n+1}| + \cdots + |A_{s+1}|.$$

We distinguish two subcases.

Case 2a. $|\hat{X}_m| + m - n \leq k$.

We have

$$\begin{aligned}
|\Delta_{mm}| &= |(2 \cdot A_m + k \cdot A) \setminus (2 \cdot A_m + k \cdot A_m)| \\
&= |(2 \cdot X_m + A) \setminus (2 \cdot X_m + A_m)| \\
&\geq |(2 \cdot X_m + (A_n \cup A_{n+1} \cup \ldots \cup A_{m-1})) \setminus (2 \cdot X_m + A_m)| \\
&\geq |A_n| + |A_{n+1}| + \cdots + |A_{m-1}|.
\end{aligned}$$

By Lemma 38, we have $|\Delta_{ii}| \geq |A_m|$, for all $i \in E$, so

$$\begin{aligned}
|2 \cdot A + k \cdot A| &= \sum_{i \in E \setminus \{m\}} |2 \cdot A_i + k \cdot A| + \sum_{i \in F \setminus \{m\}} |2 \cdot A_i + k \cdot A| \\
&\quad + |2 \cdot A_m + k \cdot A| \\
&\geq \sum_{i \in E \setminus \{m\}} (|2 \cdot A_i + k \cdot A_i| + |\Delta_{ii}|) + \sum_{i \in F \setminus \{m\}} |2 \cdot A_i + k \cdot A_i| \\
&\quad + |2 \cdot A_m + k \cdot A_m| + |\Delta_{mm}| \\
&\geq \sum_{i \in E \setminus \{m\}} [(t+1)|A_i| - 4k^{t-2}] + \sum_{i \in E \setminus \{m\}} |\Delta_{ii}| \\
&\quad + \sum_{i \in F \setminus \{m\}} [(k+2)|A_i| - 2k] \\
&\quad + (t+1)|A_m| - 4k^{t-2} + |A_n| + |A_{n+1}| + \cdots + |A_{m-1}| \\
&\geq \sum_{i \in E \cup \{m\}} [(t+1)|A_i| - 4k^{t-2}] + \sum_{i \in E \cup \{m\}} |A_i| \\
&\quad + \sum_{i \in F \setminus \{m\}} [(k+2)|A_i| - 2k] \\
&\geq (t+2)|A| - 4(|E| + |F|)k^{t-2} \geq (t+2)|A| - 4k^{t-1}.
\end{aligned}$$

Case 2b. $|\hat{X}_m| + m - n > k$.

In this case

$$|2 \cdot \hat{X}_m + \{0, u_n - u_m, \ldots, u_{m-1} - u_m\}| = k$$

and

$$|(2 \cdot X_m + (A_n \cup \ldots \cup A_m)) \setminus (2 \cdot X_m + A_n)| \geq (k - |\hat{X}_m|)|A_m|. \qquad (4.3)$$

On the other hand, we have $c_2(X_n) = c_2(A_n) = 2$, so by Proposition 31

$$\begin{aligned} |2 \cdot X_m + A_n| &= |2 \cdot X_m + k \cdot X_n| \\ &\geq 2|X_m| + |\hat{X}_m|(|X_n| - 2) \\ &= 2|A_m| + |\hat{X}_m|(|A_n| - 2). \end{aligned} \tag{4.4}$$

We have $|A_n| \geq |A_m|$. Thus, by (4.3) and (4.4),

$$\begin{aligned} |2 \cdot A_m + k \cdot A| &= |2 \cdot X_m + A| \\ &\geq |2 \cdot X_m + A_n| \\ &\quad + |2 \cdot X_m + (A_n \cup \ldots \cup A_m)) \setminus (2 \cdot X_m + A_n)| \\ &\geq 2|A_m| + |\hat{X}_m|(|A_n| - 2) + (k - |\hat{X}_m|)|A_m| \\ &\geq (k+2)|A_m| + |\hat{X}_m|(|A_n| - |A_m|) - 2k. \end{aligned}$$

By the definition of m, we have $m \leq p^{\alpha-1} + 1$, so

$$|\hat{X}_m| > k - m + n \geq k - m + 1 \geq p^\alpha - p^{\alpha-1} \geq p^{\alpha-1} \geq m - 1.$$

Thus

$$|2 \cdot A_m + k \cdot A| \geq (k+2)|A_m| + m(|A_n| - |A_m|) - 2k$$

and

$$\begin{aligned}
|2\cdot A+k\cdot A| &= \sum_{i\in E\setminus\{m\}} |2\cdot A_i+k\cdot A| \\
&\quad + \sum_{i\in F\setminus\{m\}} |2\cdot A_i+k\cdot A| + |2\cdot A_m+k\cdot A| \\
&\geq \sum_{i\in E\setminus\{m\}} (|2\cdot A_i+k\cdot A_i|+|\Delta_{ii}|) + \sum_{i\in F\setminus\{m\}} |2\cdot A_i+k\cdot A_i| \\
&\quad + (k+2)|A_m| + m(|A_n|-|A_m|) - 2k \\
&\geq \sum_{i\in E\setminus\{m\}} [(t+1)|A_i| - 4k^{t-2}] + \sum_{i\in E\setminus\{m\}} |\Delta_{ii}| \\
&\quad + \sum_{i\in F\setminus\{m\}} [(k+2)|A_i| - 2k] \\
&\quad + (k+2)|A_m| + m(|A_n|-|A_m|) - 2k \\
&\geq \sum_{i\in E\setminus\{m\}} [(t+1)|A_i| - 4k^{t-2}] + \sum_{i\in E\setminus\{m\}} |A_i| \\
&\quad + \sum_{i\in F\setminus\{m\}} [(k+2)|A_i| - 2k] + (k+2)|A_m| - 2k \\
&\geq (k+2)|A| - 4(|E|+|F|)k^{t-2} \geq (k+2)|A| - 4k^{t-1}.
\end{aligned}$$

□

Proof of Theorem 28. If $j = k$, applying Corollary 33, we obtain $|2\cdot A+k\cdot A| \geq (k+2)|A|-2k \geq (k+2)|A|-k^2-k+2$. We assume $j<k$. Without loss of generality we also assume that $\gcd(A)=1$ and $0\in A_1$. We have $|A_1| \geq \frac{|A|}{j} > 8k^{k-1}$. Let $m = \min\{1\leq i\leq j \mid p\nmid u_i\}$. We distinguish two cases.

Case 1. $E=\emptyset$.

By Corollary 33 and Lemma 34, we have

$$\begin{aligned}
|2 \cdot A + k \cdot A| &= \sum_{i=1}^{j} |2 \cdot A_i + k \cdot A| \\
&= \sum_{i=1}^{j} (|2 \cdot A_i + k \cdot A_i| + |\Delta_{ii}|) \\
&= \sum_{i=1}^{j} |2 \cdot X_i + k \cdot X_i| + \sum_{i=1}^{j} |\Delta_{ii}| \\
&\geq \sum_{i=1}^{j} [(k+2)|X_i| - 2k] + j(j-1) \\
&= (k+2)|A| - j(2k - j + 1) \\
&\geq (k+2)|A| - k^2 - k + 2.
\end{aligned}$$

Case 2. $E \neq \emptyset$.

We consider following subcases.

Case 2a. $m \in E$

By Lemma 38, we have $|\Delta_{mm}| \geq |A_1|$. Applying Lemma 39, we obtain

$$\begin{aligned}
|2 \cdot A + k \cdot A| &\geq |2 \cdot A_m + k \cdot A| + |2 \cdot (A \setminus A_m) + k \cdot (A \setminus A_m)| \\
&= |2 \cdot A_m + k \cdot A_m| + |\Delta_{mm}| + (k+2)|A \setminus A_m| - 4k^{k-1} \\
&\geq (k+2)|A_m| - 4k^{k-1} + |A_1| + (k+2)|A \setminus A_m| - 4k^{k-1} \\
&> (k+2)|A|.
\end{aligned}$$

Case 2b. $m \in F$.

If $|\Delta_{11}| \geq |A_1|$, we have

$$\begin{aligned}
|2 \cdot A + k \cdot A| &\geq |2 \cdot A_1 + k \cdot A| + |2 \cdot (A \setminus A_1) + k \cdot (A \setminus A_1)| \\
&= |2 \cdot A_1 + k \cdot A_1| + |\Delta_{11}| + (k+2)|A \setminus A_m| - 4k^{k-1} \\
&\geq (k+2)|A_1| - 4k^{k-1} + |A_1| + (k+2)|A \setminus A_m| - 4k^{k-1} \\
&> (k+2)|A|.
\end{aligned}$$

If $|\Delta_{11}| < |A_1|$, then by Lemma 37, we have $c_2(A_1) = 2$. Since $E \neq \emptyset$, there exists $s \in E$. By Lemma 38, we have $|\Delta_{ss}| \geq |A_m|$ if $p \mid u_s$ and $|\Delta_{ss}| \geq |A_1|$ if $p \nmid u_s$. Since $|A_1| \geq |A_m|$, we obtain $|\Delta_{ss}| \geq |A_m|$. We denote $A' = A \setminus (A_m \cup A_s)$. Applying Proposition 31, we obtain

$$\begin{aligned}
|2 \cdot A + k \cdot A| &\geq |2 \cdot A_m + k \cdot A| + |2 \cdot A_s + k \cdot A| + |2 \cdot A' + k \cdot A'| \\
&\geq |2 \cdot A_m + k \cdot A_1| + |2 \cdot A_s + k \cdot A_s| + |\Delta_{ss}| \\
&\quad + (k+2)|A'| - 4k^{k-1} \\
&\geq 2|A_m| + k|A_1| - 2k + (k+2)|A_s| - 4k^{k-1} + |A_m| \\
&\quad + (k+2)|A'| - 4k^{k-1} \\
&= (k+2)|A| + |A_1| - 8k^{k-1} - 2k \\
&> (k+2)|A| - 2k.
\end{aligned}$$

This ends the proof.

4.3 The case $k = pq$

Lemma 40. *Let A be a finite set of integers such that $\gcd(A) = 1$. Let $k = pq$, where p and q are distinct odd prime numbers. Let $m = \min\{1 \leq i \leq j \mid p \nmid u_i\}$ and let $i \in E$.*

(i) If $(u_2, k) = 1$, then

$$|\Delta_{ii}| \geq \begin{cases} |A_1| & \text{if } i = 2 \\ |A_2| & \text{if } i \neq 2 \end{cases}$$

(ii) If $(u_2, k) = p$, then

$$|\Delta_{ii}| \geq \begin{cases} \min\{|A_2|, q|A_m|\} & \text{if } i = 1 \\ \min\{|A_1|, q|A_m|\} & \text{if } 1 < i < m \\ |A_2| & \text{if } i = m \\ \min\{|A_1|, |A_2|, q|A_m|\} & \text{if } i > m \end{cases}$$

Proof. (i) By Lemma 35, if $i \in E$, we have $2 \cdot \hat{X}_i = 2 \cdot \hat{X}_i + u_1 \neq 2 \cdot \hat{X}_i + u_2$. Otherwise, $k \mid |\hat{X}_i|$, a contradiction. Thus, if $1 \in E$, we have

$$\begin{aligned} |\Delta_{11}| &= |(2 \cdot A_1 + k \cdot A) \setminus (2 \cdot A_1 + k \cdot A_1)| \geq |(2 \cdot X_1 + A_2) \setminus (2 \cdot X_1 + A_1)| \\ &\geq |A_2||(2 \cdot \hat{X}_1 + u_2) \setminus (2 \cdot \hat{X}_1 + u_1)| \geq |A_2|. \end{aligned}$$

Similarly, if $2 \in E$, we have $|\Delta_{11}| \geq |A_1|$.

Now, let $i \in E$ and $i \neq 1, 2$. Since $2 \cdot \hat{X}_i + u_1 \neq 2 \cdot \hat{X}_i + u_2$, we have that $2 \cdot \hat{X}_i + u_i \neq 2 \cdot \hat{X}_i + u_1$, in which case $|\Delta_{ii}| \geq |A_1|$ or $2 \cdot \hat{X}_i + u_i \neq 2 \cdot \hat{X}_i + u_2$, in which case $|\Delta_{ii}| \geq |A_2|$. In both cases $|\Delta_{ii}| \geq |A_2|$.

(ii) Let $1 \in E$. Then $2 \cdot \hat{X_1} + u_1 \neq 2 \cdot \hat{X_1} + u_2$ or $2 \cdot \hat{X_1} + u_1 = 2 \cdot \hat{X_1} + u_2$. If $2 \cdot \hat{X_1} + u_1 \neq 2 \cdot \hat{X_1} + u_2$, we obtain, as in (i), that $|\Delta_{11}| \geq |A_2|$. If $2 \cdot \hat{X_1} + u_1 = 2 \cdot \hat{X_1} + u_2$, by Lemma 35, we have that

$$2 \cdot \hat{X_1} = \bigcup_{\beta \in I} (p \cdot \{0, 1, \ldots, q-1\} + \beta)$$

for some nonempty set $I \subset \mathbb{Z}/p\mathbb{Z}$. Moreover, $p \nmid u_m$, thus $I + u_m \neq I$ and $|(2 \cdot \hat{X_1} + u_m) \setminus (2 \cdot \hat{X_1} + u_1)| \geq q$. We obtain

$$\begin{aligned} |\Delta_{11}| &= |(2 \cdot A_1 + k \cdot A) \setminus (2 \cdot A_1 + k \cdot A_1)| \geq |(2 \cdot X_1 + A_m) \setminus (2 \cdot X_1 + A_1)| \\ &\geq |A_m||(2 \cdot \hat{X_1} + u_m) \setminus (2 \cdot \hat{X_1} + u_1)| \geq q|A_m|. \end{aligned}$$

Next, if $i < m$, we have that $p \mid u_i$ and $(k, u_i) = p$. As above, we have $2 \cdot \hat{X_i} + u_i \neq 2 \cdot \hat{X_i} + u_1$ or $2 \cdot \hat{X_i} + u_i = 2 \cdot \hat{X_i} + u_1$ and we obtain $|\Delta_{ii}| \geq |A_1|$ or $|\Delta_{ii}| \geq q|A_m|$.

If $m \in E$, we have $p \nmid u_m$. Thus, $q \nmid u_m$, in which case $(k, u_m) = 1$, or $q \mid u_m$, in which case $(k, u_m - u_2) = 1$. Thus, $2 \cdot \hat{X_m} + u_m \neq 2 \cdot \hat{X_m} + u_1$ or $2 \cdot \hat{X_m} + u_m \neq 2 \cdot \hat{X_m} + u_2$. We have

$$|\Delta_{mm}| = |(2 \cdot X_m + A) \setminus (2 \cdot X_1 + A_m)| \geq |A_2|.$$

Finally, if $i > m$, we have $(k, u_i) = 1$ or $(k, u_i) = p$ or $(k, u_i) = q$. If $(k, u_i) = 1$, we have $|\Delta_{ii}| \geq |A_1|$. If $(k, u_i) = p$, we obtain $|\Delta_{ii}| \geq |A_1|$ or $|\Delta_{ii}| \geq q|A_m|$. If $(k, u_i) = q$, we have $(k, u_m - u_2) = 1$ and $|\Delta_{ii}| \geq |A_2|$.

□

Lemma 41. *Let A be a finite set of integers. If $k = pq$, where p and q*

are distinct odd primes, then

$$|2 \cdot A + k \cdot A| \geq (k+2)|A| - 4k^{k-1}.$$

Proof. Let T be the set of integers t such that for every finite set $A \subset \mathbb{Z}$

$$|2 \cdot A + k \cdot A| \geq (t+2)|A| - 4k^{t-1}.$$

As in the proof of Lemma 39, we will use induction to prove $k \in T$. By Corollary 32, we have that $2 \in T$. Let us assume that $2 \leq t \leq k$ and $t-1 \in T$. Let A be a finite set of integers. Without loss of generality we may assume that $\gcd(A) = 1$ and that $0 \in A_1$. We define $m = \min\{1 \leq i \leq j \mid p \nmid u_i\}$.

If $\sum_{i \in E} |\Delta_{ii}| \geq \sum_{i \in E} |A_i|$ the same proof holds as in Lemma 39. Let us assume that $\sum_{i \in E} |\Delta_{ii}| < \sum_{i \in E} |A_i|$. We define $n = \min\{i \in E \mid |\Delta_{ii}| < |A_i|\}$.

Case 1. $(u_2, k) = 1$. We have $2 \in F$. Otherwise, $2 \in E$ and by Lemma 40, we have $\sum_{i \in E} |\Delta_{ii}| \geq \sum_{i \in E} |A_i|$, a contradiction. Moreover, since $|\Delta_{ii}| \geq |A_2|$ for all $i \in E$, we obtain that $1 \in E$ and $|\Delta_{11}| < |A_1|$. By Lemma 37, we have $c_2(A_1) = 2$. We obtain

$$
\begin{aligned}
|2\cdot A + k\cdot A| &= \sum_{i\in E} |2\cdot A_i + k\cdot A| + \sum_{i\in F\setminus\{2\}} |2\cdot A_i + k\cdot A| \\
&\quad + |2\cdot A_2 + k\cdot A| \\
&\geq \sum_{i\in E} (|2\cdot A_i + k\cdot A_i| + |\Delta_{ii}|) + \sum_{i\in F\setminus\{2\}} |2\cdot A_i + k\cdot A_i| \\
&\quad + |2\cdot A_2 + k\cdot A_1| \\
&\geq \sum_{i\in E} [(t+1)|A_i| - 4k^{t-2}] + \sum_{i\in E} |\Delta_{ii}| \\
&\quad + \sum_{i\in F\setminus\{2\}} [(k+2)|A_i| - 2k] \\
&\quad + 2|A_2| + k|A_1| - 2k \\
&\geq \sum_{i\in E} [(t+1)|A_i| - 4k^{t-2}] + \sum_{i\in E} |A_2| \\
&\quad + \sum_{i\in F\setminus\{2\}} [(k+2)|A_i| - 2k] \\
&\quad + (k+1)|A_2| + |A_1| - 2k \\
&\geq (t+2)|A| - 4(|E| + |F|)k^{t-2} \geq (t+2)|A| - 4k^{t-1}.
\end{aligned}
$$

Case 2. $(u_2, k) = p$. Thus $m \geq 3$. By Lemma 37, we have $c_2(A_n) = 2$. By Lemma 40, we have $|\Delta_{ii}| \geq |A_m|$ for all $i \in E$. In particular $m \neq n$.

Similarly as in Lemma 39, we obtain $m > n$. We have

$$\begin{aligned}
|2 \cdot A + k \cdot A| &= \sum_{i \in E \setminus \{m\}} |2 \cdot A_i + k \cdot A| + \sum_{i \in F \setminus \{m\}} |2 \cdot A_i + k \cdot A| \\
&\quad + |2 \cdot A_m + k \cdot A| \\
&\geq \sum_{i \in E \setminus \{m\}} (|2 \cdot A_i + k \cdot A_i| + |\Delta_{ii}|) + \sum_{i \in F \setminus \{m\}} |2 \cdot A_i + k \cdot A_i| \\
&\quad + |2 \cdot X_m + A| \\
&\geq \sum_{i \in E \setminus \{m\}} (t+1)|A_i| + \sum_{i \in E \setminus \{m\}} |\Delta_{ii}| \\
&\quad + \sum_{i \in F \setminus \{m\}} (t+2)|A_i| + |2 \cdot X_m + A| \\
&\quad - (\sum_{i \in E \setminus \{m\}} 4k^{t-2} + \sum_{i \in F \setminus \{m\}} 2k).
\end{aligned}$$

If $m \in F$, using Proposition 31, we obtain

$$\begin{aligned}
|2 \cdot X_m + A| &\geq |2 \cdot X_m + A_n| = |2 \cdot X_m + k \cdot X_n| \geq 2|X_m| + k|X_n| - 2k \\
&= (k+2)|A_m| + k(|A_n| - |A_m|) - 2k.
\end{aligned}$$

Thus

$$\begin{aligned}
|2 \cdot A + k \cdot A| &\geq \sum_{i \in E} (t+1)|A_i| + \sum_{i \in E} |\Delta_{ii}| + \sum_{i \in F \setminus \{m\}} (t+2)|A_i| \\
&\quad + (t+2)|A_m| + k(|A_n| - |A_m|) - (|E|4k^{t-2} + |F|2k) \\
&\geq (t+2)|A| - 4k^{t-1}.
\end{aligned}$$

Next, let us assume $m \in E$. We have

$$|2 \cdot A + k \cdot A| \geq \sum_{i \in E \setminus \{m\}} (t+1)|A_i| + \sum_{i \in E \setminus \{m\}} |\Delta_{ii}| + \sum_{i \in F} (t+2)|A_i| + |2 \cdot X_m + A| - \Big(\sum_{i \in E \setminus \{m\}} 4k^{t-2} + \sum_{i \in F} 2k \Big). \tag{4.5}$$

If $|A_1| \leq q|A_m|$, using Lemma 40, we obtain that $1 \in E$ and

$$\sum_{i \in E} |\Delta_{ii}| \geq |A_2| + \sum_{i \in E, i \geq 2} |A_i|.$$

In particular, $|\Delta_{11}| < |A_1|$. Moreover, $2 \notin E$, otherwise, by Lemma 40, $|\Delta_{ii}| \geq |A_1|$ and $\sum_{i \in E} |\Delta_{ii}| \geq \sum_{i \in E} |A_i|$. Using the same argument as in *Case 1*, we obtain

$$|2 \cdot A + k \cdot A| \geq (t+2)|A| - 4k^{t-1}.$$

We assume $|A_1| > q|A_m|$. Then $|A_n| > q|A_m|$. Otherwise, $n \geq 2$ and by Lemma 40, we have $|\Delta_{ii}| \geq |A_n|$, for all $i \in E$ and $\sum_{i \in E} |\Delta_{ii}| \geq \sum_{i \in E} |A_i|$, a contradiction. By Lemma 40, $|\Delta_{11}| \geq \min\{|A_2|, q|A_m|\}$, $|\Delta_{ii}| \geq q|A_m|$ for all $i \in E$ such that $1 < i < m$ and $|\Delta_{ii}| \geq |A_m|$ for all $i \in E$ such that $i \geq m$. We need to consider separately the cases $|\hat{X}_m| < p$ and $|\hat{X}_m| \geq p$. Moreover, the case $|\hat{X}_m| \geq p$, we will subdivided into three subcases: $p \leq |\hat{X}_m| < q$, $|\hat{X}_m| \geq p > q$ and $|\hat{X}_m| \geq q > p$. We will use that $m \leq q + 1$.

Case 2a. $|\hat{X}_m| \geq p > q$. By Corollary 33, we have

$$\begin{aligned}|2 \cdot X_m + A| &\geq |2 \cdot X_m + A_n| \geq 2|X_m| + |\hat{X}_m||X_n| - 2k \\ &\geq (k+2)|A_m| + p(|A_n| - q|A_m|) - 2k \\ &\geq (t+2)|A_m| + (m-1)(|A_n| - q|A_m|) - 2k.\end{aligned}$$

If $n > 1$, by (4.5), we have

$$\begin{aligned}|2 \cdot A + k \cdot A| \geq & \sum_{i \in E \setminus \{m\}} (t+1)|A_i| + \sum_{i \in E \setminus \{m\}} |\Delta_{ii}| + \sum_{i \in F} (t+2)|A_i| \\ & + (t+2)|A_m| + (m-1)(|A_n| - q|A_m|) \\ & - ((|E|-1)4k^{t-2} + (|F|+1)2k) \\ \geq & (t+2)|A| - 4k^{t-1}.\end{aligned}$$

If $n = 1$, then $c_2(A_1) = 2$. We need to consider the following subcases.

If $2 \in E$, by Lemma 40, we have that $|\Delta_{11}| \geq \min\{|A_2|, q|A_m|\}$ and $|\Delta_{22}| \geq \min\{|A_1|, q|A_m|\}$, so the above proof holds.

If $2 \in F$, using Proposition 31, we obtain

$$|2 \cdot X_2 + A| \geq |2 \cdot X_2 + A_1| = |2 \cdot X_2 + k \cdot X_1| \geq 2|A_2| + k|A_1| - 2k,$$

so

$$\begin{aligned}
|2\cdot A + k\cdot A| &= \sum_{i\in E\setminus\{m\}} |2\cdot A_i + k\cdot A| + \sum_{i\in F\setminus\{2\}} |2\cdot A_i + k\cdot A| \\
&\quad + |2\cdot A_2 + k\cdot A| + |2\cdot A_m + k\cdot A| \\
&\geq \sum_{i\in E\setminus\{m\}} (|2\cdot A_i + k\cdot A_i| + |\Delta_{ii}|) + \sum_{i\in F\setminus\{2\}} |2\cdot A_i + k\cdot A_i| \\
&\quad + |2\cdot X_2 + A| + |2\cdot X_m + A| \\
&\geq \sum_{i\in E\setminus\{m\}} (t+1)|A_i| + \sum_{i\in E\setminus\{m\}} |\Delta_{ii}| + \sum_{i\in F\setminus\{2\}} (t+2)|A_i| \\
&\quad + 2|A_2| + k|A_1| + (t+2)|A_m| + (m-1)(|A_1| - q|A_m|) \\
&\quad - ((|E|-1)4k^{t-2} + (|F|+1)2k) \\
&\geq (t+2)|A| - 4k^{t-1}.
\end{aligned}$$

Case 2b. $|\hat{X}_m| \geq q > p$. Similar to the previous case, we obtain

$$\begin{aligned}
|2\cdot X_m + A| \geq |2\cdot X_m + A_n| &\geq 2|X_m| + |\hat{X}_m||X_n| - 2k \\
&\geq (k+2)|A_m| + q(|A_n| - p|A_m|) - 2k \\
&\geq (t+2)|A_m| + (m-1)(|A_n| - q|A_m|) - 2k
\end{aligned}$$

and

$$|2\cdot A + k\cdot A| \geq (t+2)|A| - 4k^{t-1}.$$

Case 2c. $|\hat{X}_m| < p$. We have $|\hat{X}_m| + m - 1 < p + q \leq pq = k$. Let $L = \{1 \leq i \leq m-1 \mid (u_i - u_m, k) \neq 1\}$. If $L = \emptyset$, then $(u_1 - u_m, k) = \cdots = (u_{m-1} - u_m, k) = 1$. Using Lemma 30, we obtain

$$|2\cdot \hat{X}_m + \{0, u_1 - u_m, \ldots, u_s - u_m\}| \geq |\hat{X}_m| + s - 1, \text{ for all } 1 \leq s \leq m-1.$$

Let $s = 1$. We have

$$|(2 \cdot \hat{X}_m + u_1) \setminus (2 \cdot \hat{X}_m + u_m)| \geq 1$$

and

$$|(2 \cdot X_m + A_1) \setminus (2 \cdot X_m + A_m)| \geq |A_1|.$$

Now, let $2 \leq s \leq m-1$ such that

$$|(2 \cdot X_m + (A_1 \cup A_2 \cup \ldots \cup A_{s-1})) \setminus (2 \cdot X_m + A_m)| \geq |A_1| + |A_2| + \cdots + |A_{s-1}|.$$

We have

$$|(2 \cdot \hat{X}_m + \{u_1, \ldots, u_{s-1}\}) \setminus (2 \cdot \hat{X}_m + u_m)| \geq s - 1$$

and

$$|(2 \cdot \hat{X}_m + \{u_1, \ldots, u_{s-1}, u_t\}) \setminus (2 \cdot \hat{X}_m + u_m)| \geq s,$$

so

$$|(2 \cdot X_m + (A_1 \cup A_2 \cup \ldots \cup A_s) \setminus (2 \cdot X_m + A_m)| \geq |A_1| + |A_2| + \cdots + |A_s|.$$

We have

$$|(2 \cdot X_m + (A_1 \cup A_2 \cup \ldots \cup A_{m-1}) \setminus (2 \cdot X_m + A_m)| \geq |A_1| + |A_2| + \cdots + |A_{m-1}|.$$

Hence,

$$\begin{aligned}
|\Delta_{mm}| &= |(2 \cdot A_m + k \cdot A) \setminus (2 \cdot A_m + k \cdot A_m)| \\
&= |(2 \cdot X_m + A) \setminus (2 \cdot X_m + X_m)| \\
&\geq |(2 \cdot X_m + (A_1 \cup A_2 \cup \ldots \cup A_m)) \setminus (2 \cdot X_m + A_m)| \\
&\geq |A_1| + |A_2| + \cdots + |A_{m-1}|
\end{aligned}$$

and

$$|2 \cdot A_m + k \cdot A| \geq |2 \cdot A_m + k \cdot A_m| + |\Delta_{mm}|$$
$$\geq (t+1)|A_m| + |A_1| + |A_2| + \cdots + |A_{m-1}| - 4k^{t-2}.$$

Using (4.5), we obtain

$$|2 \cdot A + k \cdot A| \geq \sum_{i \in E}(t+1)|A_i| + \sum_{i \in E \setminus \{m\}} |\Delta_{ii}| + \sum_{i \in F}(t+2)|A_i|$$
$$+ |A_1| + |A_2| + \cdots + |A_{m-1}| - (|E|4k^{t-2} + |F|2k)$$
$$\geq (t+2)|A| - 4k^{t-1}.$$

Now, let us assume that $L \neq \emptyset$. Thus there exists $1 \leq l \leq m-1$ such that $(u_l - u_m, k) \neq 1$. Since $p \mid u_l$ and $p \nmid u_m$, we obtain that $(u_l - u_m, k) = q$. Thus $|L| = 1$. Since $|\hat{X}_m| < p$, by Lemma 35, we have $|\hat{X}_m + (u_l - u_m) \setminus \hat{X}_m| \geq 1$. Then, using Lemma 30 and Lemma 36, we obtain

$$|2 \cdot \hat{X}_m + \{0, u_1 - u_m, \ldots, u_s - u_m\}| \geq |\hat{X}_m| + s - 1, \text{ for all } 1 \leq s \leq m-1.$$

Similarly as in the case $L = \emptyset$, we have

$$|(2 \cdot X_m + (A_1 \cup A_2 \cup \ldots \cup A_m) \setminus (2X_m + A_m)| \geq |A_1| + |A_2| + \cdots + |A_{m-1}|$$

and

$$|2 \cdot A + k \cdot A| \geq (t+2)|A| - 4k^{t-1}.$$

Case 2d. $p \leq |\hat{X}_m| < q$. Let $(X_m)_q = \{x \pmod q \mid q \in X_m\}$. Then $|(X_m)_q| \leq |\hat{X}_m| < q$. Moreover, $(u_i, q) = 1$, for $2 \leq i \leq m-1$ and $|\{u_i \pmod q \mid 2 \leq i \leq m-1\}| = m-2$, so by Lemma 30

$$|2 \cdot (X_m)_q + \{u_1 \pmod q, u_2 \pmod q, \ldots, u_t \pmod q\}| \geq \min\{q, |(X_m)_q| + s - 1\}$$

for all $1 \leq s \leq m-1$. Similarly, as in the previous case, we have

$$|(X_m + (A_1 \cup A_2 \cup \cdots \cup A_m) \setminus (X_m + A_1)| \geq |A_2| + \cdots + |A_r|,$$

where $r = \min\{m-1, q+1-(X_m)_q\}$. We obtain

$$\begin{aligned} |2 \cdot X_m + A| &\geq |2 \cdot X_m + A_1| + |(X_m + (A_1 \cup A_2 \cup \cdots \cup A_m) \setminus (X_m + A_1)| \\ &\geq c_2(A_1)|X_m| + |\hat{X}_m||A_1| + |A_2| + \cdots + |A_r| - 2k. \end{aligned}$$

We have two subcases: $|\Delta_{11}| \geq |A_1|$ or $|\Delta_{11}| < |A_1|$ and $c_2(A_1) = 2$. In both subcases, using Lemma 40, we obtain

$$\begin{aligned} |2 \cdot A + k \cdot A| = & \sum_{i \in E \setminus \{m\}} |2 \cdot A_i + k \cdot A| + |2 \cdot A_m + k \cdot A| \\ & + \sum_{i \in F} |2 \cdot A_i + k \cdot A| \\ \geq & \sum_{i \in E \setminus \{m\}} |2 \cdot A_i + k \cdot A_i| + \sum_{i \in E \setminus \{m\}} |\Delta_{ii}| + |2 \cdot X_m + A| \\ & + \sum_{i \in F, i \leq m-1} |2 \cdot A_i + k \cdot A_n| + \sum_{i \in F, i > m} |2 \cdot A_i + k \cdot A_i| \\ \geq & \sum_{i \in E \setminus \{m\}} ((t+1)|A_i| - 4k^{t-1}) \\ & + |\Delta_{11}| + \sum_{i \in E, 2 \leq i \leq m-1} q|A_m| + \sum_{i \in E, m+1 \leq i \leq j} |A_m| \\ & + \sum_{i \in F, i \leq m-1} (2|A_i| + k|A_n| - 2k) + \sum_{i \in F, i > m} ((k+2)|A_i| - 2k) \\ & + c_2(A_1)|X_m| + |\hat{X}_m||A_1| + |A_2| + \cdots + |A_r| - 2k \end{aligned}$$

$$
\begin{aligned}
&\geq \sum_{i\in E\setminus\{m\}} (t+1)|A_i| + \sum_{i\in E, 2\leq i\leq m-1} q|A_m| + \sum_{i\in E, m+1\leq i\leq j} |A_m| \\
&\quad + \sum_{i\in F, i\leq m-1} (2|A_i| + k|A_n|) + \sum_{i\in F, i>m} (k+2)|A_i| \\
&\quad + 2|X_m| + |\hat{X}_m||A_1| + |A_2| + \cdots + |A_r| - 2k \\
&\quad - ((|E|-1)4k^{t-2} + (|F|+1)2k) \\
&\geq \sum_{i\in E\setminus\{m\}} (t+2)|A_i| + \sum_{i\in F} (t+2)|A_i| + 2|A_m| \\
&\quad + (|\hat{X}_m| - m + r)|A_1| \\
&\quad + (m-2)q|A_m| - ((|E|-1)4k^{t-2} + (|F|+1)2k) \\
&\geq \sum_{i\in (E\cup F)\setminus\{m\}} (t+2)|A_i| + 2|A_m| + (|\hat{X}_m| + r - 2)q|A_m| \\
&\quad - ((|E|-1)4k^{t-2} + (|F|+1)2k).
\end{aligned}
$$

By the definition of r, we have

$$
\begin{aligned}
|\hat{X}_m| + r - 2 &\geq \min\{|\hat{X}_m| + m - 3, |\hat{X}_m| + q - 1 - (X_m)_q\} \\
&\geq \min\{|\hat{X}_m| + m - 3, q - 1\} \geq p.
\end{aligned}
$$

Thus

$$
|2\cdot A + k\cdot A| \geq (t+2)|A| - 4k^{t-1}.
$$

□

Proof of Theorem 29. If $j = k$, applying Corollary 33, we obtain $|2\cdot A + k\cdot A| \geq (k+2)|A| - 2k \geq (k+2)|A| - k^2 - k + 2$. We assume $j < k$.

Without loss of generality we also assume that $\gcd(A) = 1$ and $0 \in A_1$. We have $|A_1| \geq \frac{|A|}{j} > 8k^{k-1}$. Let $m = \min\{1 \leq i \leq j \mid p \nmid u_i\}$.

The proof in the case $E = \emptyset$ is the same as the proof of this case in Theorem 28. We assume $E \neq \emptyset$.

If $|\Delta_{11}| \geq |A_1|$, we have

$$\begin{aligned}
|2 \cdot A + k \cdot A| &\geq |2 \cdot A_1 + k \cdot A| + |2 \cdot (A \setminus A_1) + k \cdot (A \setminus A_1)| \\
&= |2 \cdot A_1 + k \cdot A_1| + |\Delta_{11}| + (k+2)|A \setminus A_1| - 4k^{k-1} \\
&\geq (k+2)|A_1| - 4k^{k-1} + |A_1| + (k+2)|A \setminus A_1| - 4k^{k-1} \\
&> (k+2)|A|.
\end{aligned}$$

We assume $|\Delta_{11}| < |A_1|$. Then by Lemma 37, we have $c_2(A_1) = 2$. We consider following cases.

Case 1. $(u_2, k) = 1$

Let $2 \in F$. Since $E \neq \emptyset$, there exists $s \in E$. By Lemma 40, we have $|\Delta_{ss}| \geq |A_2|$. We denote $A' = A \setminus (A_2 \cup A_s)$. We obtain

$$\begin{aligned}
|2\cdot A + k\cdot A| &\geq |2\cdot A_2 + k\cdot A| + |2\cdot A_s + k\cdot A| + |2\cdot A' + k\cdot A'| \\
&\geq |2\cdot A_2 + k\cdot A_1| + |2\cdot A_s + k\cdot A_s| + |\Delta_{ss}| \\
&\quad + (k+2)|A'| - 4k^{k-1} \\
&\geq 2|A_2| + k|A_1| - 2k + (k+2)|A_s| - 4k^{k-1} + |A_2| \\
&\quad + (k+2)|A'| - 4k^{k-1} \\
&\geq (k+2)|A| + |A_1| - 8k^{k-1} - 2k \\
&> (k+2)|A| - 2k.
\end{aligned}$$

If $2 \in E$, then by Lemma 40, we have $|\Delta_{22}| \geq |A_1|$. Thus

$$\begin{aligned}
|2\cdot A + k\cdot A| &\geq |2\cdot A_2 + k\cdot A| + |2\cdot (A\setminus A_2) + k\cdot (A\setminus A_2)| \\
&= |2\cdot A_2 + k\cdot A_2| + |\Delta_{22}| + (k+2)|A\setminus A_2| - 4k^{k-1} \\
&\geq (k+2)|A_2| - 4k^{k-1} + |A_1| + (k+2)|A\setminus A_2| - 4k^{k-1} \\
&\geq (k+2)|A| + |A_1| - 8k^{k-1} \\
&> (k+2)|A|.
\end{aligned}$$

Case 2. $(u_2, k) = p$. We consider the following subcases.

Case 2a. $m \in F$. Since $E \neq \emptyset$, there exists $s \in E$. By Lemma 40, we

have $|\Delta_{ss}| \geq |A_m|$. We denote $A' = A \setminus (A_m \cup A_s)$. We obtain

$$\begin{aligned}
|2 \cdot A + k \cdot A| &\geq |2 \cdot A_m + k \cdot A| + |2 \cdot A_s + k \cdot A| + |2 \cdot A' + k \cdot A'| \\
&\geq |2 \cdot A_m + k \cdot A_1| + |2 \cdot A_s + k \cdot A_s| + |\Delta_{ss}| \\
&\quad + (k+2)|A'| - 4k^{k-1} \\
&\geq 2|A_m| + k|A_1| - 2k + (k+2)|A_s| - 4k^{k-1} + |A_m| \\
&\quad + (k+2)|A'| - 4k^{k-1} \\
&\geq (k+2)|A| + |A_1| - 8k^{k-1} - 2k \\
&> (k+2)|A| - 2k
\end{aligned}$$

Case 2b. $m \in E$. Here we will consider separate cases when $|\hat{X}_m| \geq p$ and $|\hat{X}_m| < p$. Moreover, the case $|\hat{X}_m| \geq p$ we will divide in two subcases: $|A_1| \leq q|A_m|$ and $|A_1| > q|A_m|$.

First we assume that $|\hat{X}_m| \geq p$ and $|A_1| \leq q|A_m|$.

Let $2 \in F$. By Lemma 40, we have $|\Delta_{mm}| \geq |A_2|$. We denote $A' = A \setminus (A_2 \cup A_m)$. We obtain

$$\begin{aligned}
|2 \cdot A + k \cdot A| &\geq |2 \cdot A_2 + k \cdot A| + |2 \cdot A_m + k \cdot A| + |2 \cdot A' + k \cdot A'| \\
&\geq |2 \cdot A_2 + k \cdot A_1| + |2 \cdot A_m + k \cdot A_m| + |\Delta_{mm}| \\
&\quad + (k+2)|A'| - 4k^{k-1} \\
&\geq 2|A_2| + k|A_1| - 2k + (k+2)|A_m| - 4k^{k-1} + |A_2| \\
&\quad + (k+2)|A'| - 4k^{k-1} \\
&\geq (k+2)|A| + |A_1| - 8k^{k-1} - 2k \\
&> (k+2)|A| - 2k.
\end{aligned}$$

If $2 \in E$, by Lemma 40, we have $|\Delta_{22}| \geq |A_1|$. Thus

$$\begin{aligned}
|2 \cdot A + k \cdot A| &\geq |2 \cdot A_2 + k \cdot A| + |2 \cdot (A \setminus A_2) + k \cdot (A \setminus A_2)| \\
&= |2 \cdot A_2 + k \cdot A_2| + |\Delta_{22}| + (k+2)|A \setminus A_2| - 4k^{k-1} \\
&\geq (k+2)|A_2| - 4k^{k-1} + |A_1| + (k+2)|A \setminus A_2| - 4k^{k-1} \\
&\geq (k+2)|A| + |A_1| - 8k^{k-1} \\
&> (k+2)|A|.
\end{aligned}$$

Next we assume that $|\hat{X}_m| \geq p$ and $|A_1| > q|A_m|$. By Corollary 33, we have

$$|2 \cdot X_m + A| \geq |2 \cdot X_m + A_1| \geq 2|X_m| + |\hat{X}_m||X_1| - 2k.$$

If $|\hat{X}_m| > p$, we obtain

$$|2 \cdot X_m + A| \geq |2 \cdot X_m + A_1| \geq 2|A_m| + (p+1)|A_1| - 2k. \tag{4.6}$$

If $|\hat{X}_m| = p$, by Lemma 35, we have $|(2 \cdot \hat{X}_m + u_2) \setminus (2 \cdot \hat{X}_m + u_1)| \geq 1$ and

$$|(2 \cdot X_m + A_2) \setminus (2 \cdot X_m + A_1)| \geq |A_2||(2 \cdot \hat{X}_m + u_2) \setminus (2 \cdot \hat{X}_m + u_1)| \geq |A_2|.$$

Thus

$$\begin{aligned}
|2 \cdot X_m + A| &\geq |2 \cdot X_m + A_1| + |(2 \cdot X_m + A_2) \setminus (2 \cdot X_m + A_1)| \qquad (4.7) \\
&\geq |2 \cdot X_m + A_1| + |A_2| \geq 2|A_m| + p|A_1| + |A_2| - 2k.
\end{aligned}$$

Now, let $2 \in F$. We denote $A' = A \setminus (A_2 \cup A_m)$. We have

$$\begin{aligned}
|2 \cdot A + k \cdot A| &\geq |2 \cdot A_2 + k \cdot A| + |2 \cdot A_m + k \cdot A| + |2 \cdot A' + k \cdot A'| \\
&\geq |2 \cdot A_2 + k \cdot A_1| + |2 \cdot A_m + k \cdot A_m| + |\Delta_{mm}| \\
&\quad + (k+2)|A'| - 4k^{k-1} \\
&\geq 2|A_2| + k|A_1| - 2k + (k+2)|A_m| + |A_2| - 4k^{k-1} \\
&\quad + (k+2)|A'| - 4k^{k-1} \\
&\geq (k+2)|A| + |A_1| - 8k^{k-1} - 2k \\
&> (k+2)|A| - 2k.
\end{aligned}$$

If $2 \in E$, by Lemma 40, we have $|\Delta_{22}| \geq q|A_m|$. Thus, if $A' = A \setminus (A_2 \cup A_m)$, then

$$\begin{aligned}
|2 \cdot A + k \cdot A| &\geq |2 \cdot A_2 + k \cdot A| + |2 \cdot A_m + k \cdot A| + |2 \cdot A' + k \cdot A'| \\
&\geq |2 \cdot A_2 + k \cdot A_2| + |\Delta_{22}| + |2 \cdot X_m + A| \\
&\quad + (k+2)|A'| - 4k^{k-1} \\
&\geq (k+2)|A_2| - 4k^{k-1} + q|A_m| + 2|A_m| + p|A_1| + |A_2| - 2k \\
&\quad + (k+2)|A'| - 4k^{k-1} \\
&\geq (k+2)|A_2| + (k+2)|A'| + q|A_m| + 2|A_m| \\
&\quad + (p-1)q|A_m| + |A_1| - 8k^{k-1} - 2k \\
&\geq (k+2)|A| + |A_1| - 8k^{k-1} - 2k \\
&> (k+2)|A| - 2k
\end{aligned}$$

Finally, we assume that $|\hat{X}_m| < p$. By Lemma 35, we have $|(2 \cdot \hat{X}_m + u_1) \setminus$

$(2 \cdot \hat{X}_m + u_m)| \geq 1$ and

$|\Delta_{mm}| \geq |(2 \cdot X_m + A_1) \setminus (2 \cdot X_m + A_m)| \geq |A_1||(2 \cdot \hat{X}_m + u_2) \setminus (2 \cdot \hat{X}_m + u_1)| \geq |A_1|$.

Thus

$$\begin{aligned}
|2 \cdot A + k \cdot A| &\geq |2 \cdot A_m + k \cdot A| + |2 \cdot (A \setminus A_m) + k \cdot (A \setminus A_m)| \\
&= |2 \cdot A_m + k \cdot A_m| + |\Delta_{mm}| + (k+2)|A \setminus A_m| - 4k^{k-1} \\
&\geq (k+2)|A_m| - 4k^{k-1} + |A_1| + (k+2)|A \setminus A_m| - 4k^{k-1} \\
&\geq (k+2)|A| + |A_1| - 8k^{k-1} \\
&> (k+2)|A|.
\end{aligned}$$

This ends the proof.

Bibliography

[1] P. T. Bateman and P. Erdős, *Monotonicity of partition functions*, Mathematika **3** (1956), 1–14.

[2] A. Biró, *Divisibility of integer polynomials and tilings of the integers*, Acta Arith. 118 (2005), no. 2, 117–127.

[3] B. Bukh, *Sums of dilates*, Combinatorics, Probability and Computing, vol. 17 (2008)

[4] E. R. Canfield and H. S. Wilf, *On the growth of restricted integer partition functions*, arXiv:1009.4404, 2010.

[5] J. Cilleruelo, Y. O. Hamidoune, O. Serra, *On sums of dilates*, Combinatorics, Probability and Computing (2009) 18, 871880.

[6] J. Cilleruelo, M. Silva, C. Vinuesa, *A sumset problem*, Journal of Combinatorics and Number Theory, 2 (2010).

[7] S-S. Du, H.-Q. Cao, Z.-W. Sun, *On a sumset problem for integers*, arXiv:1011.5438

[8] V. A. Efremovič, The proximity geometry of Riemannian manifolds, Uspekhi Mat. Nauk 8 (1953), 189.

[9] R. Grigorchuk and I. Pak, *Groups of intermediate growth: an introduction*, Enseign. Math. (2) **54** (2008), no. 3-4, 251–272.

[10] Y. O. Hamidoune and J. Rué, *A Lower Bound for the Size of a Minkowski Sum of Dilates*, Combinatorics, Probability and Computing (2010).

[11] P. de la Harpe, *Topics in Geometric Group Theory*, Chicago Lectures in Mathematics, University of Chicago Press, Chicago, IL, 2000.

[12] R. Jin, L. A. Borisov, *Finding integral diagonal pairs in a two dimensional $\mathcal{N}$–set* , arXiv:1007.1441.

[13] Ž. Ljujić, C. Sanabria, *A note on an inverse problem for lattice points*, Topology and its Applications, Volume 158, Issue 8, 2011,1012-1018

[14] Ž. Ljujić, M. B. Nathanson, *On a partition problem of Canfield and Wilf*, arXiv:1101.0599

[15] Ž. Ljujić, *Periodicity of complementing multisets*, arXiv:1010.6107 (accepted for publication in Functiones et Approximatio Commentarii Mathematici)

[16] M. N. Kolountzakis, *Translational tilings of the integers with long periods*, Electron. J. Combin. 10 (2003), Research Paper 22, 9 pp. (electronic).

[17] J. Milnor, A note on curvature and fundamental group, J. Differential Geometry 2 (1968), 1–7.

[18] M. B. Nathanson, Additive Number Theory: Inverse Problems and Geometry of Sumsets, Graduate Text in Mathematics 165, Springer-Verlag, Berlin Heidelberg New York, 1996.

[19] M. B. Nathanson, An inverse problem in number theory and geometric group theory, in: D. Chudnovsky and G. Chudnovsky, editors, *Additive Number Theory*, Springer, New York, 2010 (available on arXiv:0901.1458).

[20] M. B. Nathanson, K. O'Bryant, B. Orosz, I. Ruzsa, and M. Silva, *Binary linear forms over finite set of integers*, Acta Arith., 129: 341-361, 2007, arXiv:math/0701001

[21] M. B. Nathanson, *Elementary Methods in Number Theory*, Graduate Texts in Mathematics, vol. 195, Springer-Verlag, New York, 2000.

[22] M. B. Nathanson, *Inverse problems for linear forms over finite sets of integers*, J. Ramanujan Math. Soc. 23 (2008), 151–165.

[23] M. B. Nathanson, *Partitions with parts in a finite set*, Proc. Amer. Math. Soc. **128** (2000), no. 5, 1269–1273.

[24] M. B. Nathanson, *Phase transitions in infinitely generated groups, and related problems in additive number theory*, Integers **11** (2011), to appear.

[25] M. B. Nathanson, *Problems in additive number theory, II: Linear forms and complementing sets of integers*, Journal de Théorie des Nombres de Bordeaux, 21 no.2 (2009), pp. 343–355.

[26] D. J. Newman, *Tesselation of integers*, J. Number Theory 9 (1977), no. 1, 10–111.

[27] I. Schur, *Zur additiven Zahlentheorie*, Sitzungsber. der preuss. Akad. der Wiss., Math. Phys. Klasse (1926), 488–495.

[28] A. S. Švarc, A volume invariant of coverings, Dokl. Akad. Nauk SSSR (N.S.) 105 (1955), 3234.

[29] R. Tijdeman, *Periodicity and almost-periodicity, More Sets, Graphs and Numbers*, Bolyai Soc. Math. Stud., vol. 15, Springer, Berlin, 2006, pp. 381–405.