Contributions to Discrete Mathematics

Volume 20, Number 1, Pages 42–59
ISSN 1715-0868

ON THE FREIMAN–LEV CONJECTURE

YUJIE WANG AND MIN TANG

Abstract. Let A be a set of k integers such that $A \subseteq [0,l]$, $0, l \in A$ and $\gcd(A) = 1$. Let $2^\wedge A$ denote the set of all sums of two distinct elements of A. Write $W = \{w \in [0,l] \backslash A : w, w+l \notin 2^\wedge A\}$. In this paper, we obtain the upper bound of $|W|$ with some restrictions on l. As an application, we show that the Freiman–Lev conjecture is true for $l = 2k-4$ using the structure of A with $|W| = 2$.

1. Introduction

Let A be a finite set of integers. Let $2A$ and $2^\wedge A$ denote the set of all sums of two elements of A and the set of all sums of two distinct elements of A, respectively. Define the interval of integers $[m,n] = \{x \in \mathbb{Z} \mid m \leqslant x \leqslant n\}$ and $\gcd(A)$ the greatest common divisor of all nonzero elements of A. For integer a and positive integer m, let $a \pmod m$ be the least nonnegative residue of a modulo m.

In 1959, Freiman [2] proved the following result (see also [5])

Theorem A. *Let $k \geqslant 3$. Let A be a finite set of k integers such that $A \subseteq [0,l]$, $0, l \in A$ and $\gcd(A) = 1$. Then*

$$|2A| \geqslant \begin{cases} l+k, & \text{if } l \leqslant 2k-3, \\ 3k-3, & \text{if } l \geqslant 2k-2. \end{cases}$$

In 1999, Freiman, Low, and Pitman [3] obtained the following theorem by using some combinatorial arguments together with Freiman's theorem on $2A$.

Theorem B. *Let A be a set of $k \geq 2$ integers for which*

$$|2^\wedge A| \leq 2k-3+C,$$

where $0 \leq C \leq \frac{1}{2}(k-5)$. Then A is contained in an arithmetic progression L such that $|L| \leq k+2C+2$.

Received by the editors August 17, 2022, and in revised form March 18, 2023.

2000 *Mathematics Subject Classification.* 11B13.

Key words and phrases. restricted sumsets; Freiman–Lev conjecture.

This work was supported by the National Natural Science Foundation of China(Grant Nos. 12371003 and 12101007) and the Natural Science Foundation of Anhui Province (Grant No. 2008085QA06).

In [4], Lev remarked that the following conjecture was posed by Freiman (through personal communication) and independently by himself.

Conjecture. *Let A be a set of $k > 7$ integers such that $A \subseteq [0, l]$, $0, l \in A$ and* $\gcd(A) = 1$. *Then*

$$|2^\wedge A| \geqslant \begin{cases} l + k - 2, & \text{if } l \leqslant 2k - 5, \\ 3k - 7, & \text{if } l \geqslant 2k - 4. \end{cases}$$

Lev [4] showed that the Freiman–Lev conjecture holds if l is a prime number. Moreover, he obtained a result nearer to the above conjecture.

Theorem C. *Let A be a set of $k \geqslant 3$ integers such that $A \subseteq [0, l]$, $0, l \in A$ and* $\gcd(A) = 1$. *Then*

$$|2^\wedge A| \geqslant \begin{cases} l + k - 2, & \text{if } l \leqslant 2k - 5, \\ (\theta + 1)k - 6, & \text{if } l \geqslant 2k - 4, \end{cases}$$

where $\theta = (1 + \sqrt{5})/2$.

After this, Ruzsa [6], Bourgain [1] and Schoen [7] almost solved the conjecture of Freiman and Lev.

Theorem D. *Let A be a set of $k > 7$ integers such that $A \subseteq [0, l]$, $0, l \in A$ and* $\gcd(A) = 1$. *Then*

$$|2^\wedge A| \geqslant \begin{cases} l + k - 2, & \text{if } l \leqslant 2k - 5, \\ 3k + o(k), & \text{if } l \geqslant 2k - 4. \end{cases}$$

Recently, the second author of this paper and Wang [9] gave a solution to the Freiman–Lev conjecture in the cases of sets with a specific diameter.

Theorem E. *Let A be a set of $k \geqslant 5$ integers such that $A \subseteq [0, l]$, $0, l \in A$ and* $\gcd(A) = 1$. *Then*

(1) if $l = 2k - 3$, then $|2^\wedge A| \geqslant 3k - 7$.
(2) if $l = 2k - 4$, then $|2^\wedge A| \geqslant 3k - 8$.
(3) if $l = 2k - 4 = 2^s (s \geqslant 1)$, then $|2^\wedge A| \geqslant 3k - 7$.

Let A be a set of k integers such that $A \subseteq [0, l]$, $0, l \in A$ and $\gcd(A) = 1$. For any integer w, let

$$S(w) = \{w, w + l\}.$$

The following fact about $S(w)$ is the key point in the proof of the Freiman–Lev conjecture with $l \leqslant 2k - 5$ (See Theorem 2.1 [8]).

Fact A. Let A be a set of $k \geqslant 5$ such that $A \subseteq [0, l]$, $0, l \in A$ and $\gcd(A) = 1$. If $l \leqslant 2k - 5$, then

$$S(w) \cap 2^\wedge A \neq \emptyset$$

for all integers $w \in [0, l] \backslash A$.

If $l \geqslant 2k - 4$, there may exist some elements $w \in [0, l] \backslash A$ such that w and $w + l$ don't belong to $2^\wedge A$. We denote these "*bad*" elements by the set

$$W = \{w \in [0, l] \backslash A \mid S(w) \cap 2^\wedge A = \emptyset\}.$$

In this paper, we find a strong upper bound of $|W|$.

Theorem 1.1. *Let A be a set of $k \geqslant 5$ integers such that $A \subseteq [0, l]$, $0, l \in A$ and* $\gcd(A) = 1$. *If $l \leqslant 2k-3$, then $|W| \leqslant 2$.*

Moreover, we give the structure of A with $|W| = 2$.

Proposition 1.2. *Let A be a set of $k > 7$ integers such that $A \subseteq [0, l]$, $0, l \in A$ and $l \leqslant 2k-3$. Let $W = \{w_1, w_2\}$ with* $\gcd(w_2 - w_1, l) = m$. *Write $V := \left\{\frac{w_2}{2}, \frac{w_2+l}{2}\right\} \cap \mathbb{Z}$. Fix an integer $v \in V$, for any integer $x \in \left[0, \frac{l}{m} - 1\right]$, let $q(x)$ be the integer such that $0 \leq v + x(w_2 - w_1) - q(x)l < l$. Write $r_v(x) := v + x(w_2 - w_1) - q(x)l$. Define*

$$\mathcal{D}^-(v) := \left\{ r_v(x) : x \in \left[0, \frac{l}{2m} - \frac{1}{2}\right] \right\},$$

$$\mathcal{D}^+(v) := \left\{ r_v(x) : x \in \left[\frac{l}{2m} + \frac{1}{2}, \frac{l}{m} - 1\right] \right\}.$$

Then

(1) $\mathcal{D}^-(v) \subseteq A$ for all $v \in V$;
(2) $\mathcal{D}^+(v) \cap A = \emptyset$ for all $v \in V$;
(3) If $v \equiv 0 \pmod{m}$ for some $v \in V$, then $0 \in \mathcal{D}^-(v)$.

Proposition 1.3. *Let A be a set of $k > 7$ integers such that $A \subseteq [0, l]$, $0, l \in A$ and $l \leqslant 2k-3$. Let $W = \{w_1, w_2\}$ with* $\gcd(w_2 - w_1, l) = m$. *For any integer $x \in \left[0, \frac{l}{m} - 1\right]$, let $q(x)$ be the integer such that $0 \leq x(w_2 - w_1) - q(x)l < l$. Write $r(x) := x(w_2 - w_1) - q(x)l$. Define*

$$H := \left\{ r(x) : x \in \left[0, \frac{l}{m} - 1\right] \right\}.$$

If $u \in [0, m-1] \cap A$ and $2u \not\equiv w_2 \pmod{m}$, then $u + H \subseteq A$.

Proposition 1.4. *Let A be a set of $k > 7$ integers such that $A \subseteq [0, l]$, $0, l \in A$ and $l \leqslant 2k-3$. Let $w_1, w_2 \in W$ with* $\gcd(w_2 - w_1, l) = m$. *Write $V := \left\{\frac{w_2}{2}, \frac{w_2+l}{2}\right\} \cap \mathbb{Z}$. Then*

$$A = \{l\} \cup (U + H) \cup \bigcup_{v \in V} \mathcal{D}^-(v),$$

where $U = \{u \in [0, m-1] \cap A : 2u \not\equiv w_2 \pmod{m}\}$, $H = m\mathbb{Z} \cap [0, l)$ is defined as in Proposition 1.3 and $\mathcal{D}^-(v)$ is defined as in Proposition 1.2.

Using the structure of A with $|W| = 2$, we prove that the Freiman–Lev conjecture holds for $2k-4 \leqslant l \leqslant 2k-3$. (For $l = 2k-3$, see Theorem E [9]. Here we give a new proof.)

Theorem 1.5. *Let A be a set of $k > 7$ integers such that $A \subseteq [0, l]$, $0, l \in A$ and* $\gcd(A) = 1$. *If $2k-4 \leqslant l \leqslant 2k-3$, then $|2^\wedge A| \geqslant 3k-7$.*

2. Proof of Theorem 1.1.

Lemma 2.1. *Let A be a set of $k \geqslant 5$ integers such that $A \subseteq [0,l]$, $0, l \in A$,* $\gcd(A) = 1$ *and $l \leqslant 2k-3$. For any $w \in W$, we have*

(1) $|S(w) \cap 2A| = 2$ if and only if $l = 2k-4$. In this case, w is even and $\{\frac{w}{2}, \frac{w+l}{2}\} \subseteq A$;

(2) $|S(w) \cap 2A| = 1$ if and only if $l = 2k-3$. In this case, $\frac{w}{2} \in A$ for w is even and $\frac{w+l}{2} \in A$ for w is odd.

Proof. By Fact A, we know that $W = \emptyset$ if $l \leq 2k-5$. Since $l \leq 2k-3$ and $w \in W$, we have

$$l = 2k-4 \text{ or } 2k-3. \tag{2.1}$$

By the proof of Theorem A (See Theorems 1.13 and 1.14 of [5]), if $l \leqslant 2k-3$, then $S(w) \cap 2A \neq \emptyset$, thus

$$|S(w) \cap 2A| = 1 \text{ or } 2. \tag{2.2}$$

We will make use of the following decompositions

$$[0,w] = \bigcup_{i=0}^{\lfloor \frac{w}{2} \rfloor} \{i, w-i\}, \quad [w+1, l] = \bigcup_{i=1}^{\lfloor \frac{l-w}{2} \rfloor} \{w+i, l-i\} \cup \{l\}. \tag{2.3}$$

Since $w, w+l \notin 2^\wedge A$, we have

$$|\{i, w-i\} \cap A| \leqslant 1, \quad i = 0, 1, \dots, \left\lfloor \frac{w}{2} \right\rfloor - 1, \tag{2.4}$$

$$|\{i, w+l-i\} \cap A| \leqslant 1, \quad i = w+1, w+2, \dots, w + \left\lfloor \frac{l-w}{2} \right\rfloor - 1. \tag{2.5}$$

(1) If $|S(w) \cap 2A| = 2$, then $w, w+l \in 2A \setminus 2^\wedge A$. Therefore, we have $\frac{w}{2}, \frac{w+l}{2} \in A$, thus w, l are even. Hence $l = 2k-4$.

On the other hand, assume that $l = 2k-4$, we shall show that $|S(w) \cap 2A| = 2$.

In fact, if $\frac{w}{2} \in A$ and $\frac{w+l}{2} \notin A$, then by (2.3)–(2.5), we have

$$|[0,w] \cap A| \leqslant \frac{w}{2} + 1, \quad |[w+1, l] \cap A| \leqslant \frac{l-w}{2}. \tag{2.6}$$

If $\frac{w}{2} \notin A$ and $\frac{w+l}{2} \in A$, then as l is even, and $w+l$ must be even, w is also even. Thus, by (2.3)–(2.5), we have

$$|[0,w] \cap A| \leqslant \frac{w}{2}, \quad |[w+1, l] \cap A| \leqslant \frac{l-w}{2} + 1. \tag{2.7}$$

By (2.6) and (2.7), in either of the above cases we have

$$k = |A| \leqslant \frac{w}{2} + 1 + \frac{l-w}{2} \leqslant \frac{l}{2} + 1 = k-1,$$

a contradiction.

Hence, $|S(w) \cap 2A| = 2$ if and only if $l = 2k-4$.

(2) By (2.1), (2.2) and (1), we can obtain that $|S(w)\cap 2A| = 1$ if and only if $l = 2k-3$.

This completes the proof of Lemma 2.1. □

Lemma 2.2. *Let A be a set of $k \geqslant 5$ integers such that $A \subseteq [0,l]$, $0, l \in A$, $\gcd(A) = 1$ and $l \leqslant 2k-3$. For any $w \in W$, we have*

(1) If $i \in A\backslash\{\frac{w}{2}, \frac{w+l}{2}\}$, then $|S(w-i)\cap A| = 0$;

(2) If $i \in [0,l]\backslash A$ or $i \in A \cap \{\frac{w}{2}, \frac{w+l}{2}\}$, then $|S(w-i)\cap A| = 1$.

Proof. By (2.3)–(2.5), if $l = 2k-4$, then

$$|[0,w]\cap A| \leqslant \frac{w}{2}+1, \quad |[w+1,l]\cap A| \leqslant \frac{l-w}{2}+1$$

and if $l = 2k-3$, then

$$|[0,w]\cap A| \leqslant \begin{cases} \frac{w}{2}+1, & w \text{ is even,} \\ \frac{w+1}{2}, & w \text{ is odd,} \end{cases}$$

$$|[w+1,l]\cap A| \leqslant \begin{cases} \frac{l-w+1}{2}, & w \text{ is even,} \\ \frac{l-w}{2}+1, & w \text{ is odd.} \end{cases}$$

By the above cases and a trivial fact

$$k = |A| = |[0,w]\cap A| + |[w+1,l]\cap A|,$$

we have

$$|\{i, w-i\}\cap A| = 1, \quad 1 \leqslant i \leqslant w-1, \tag{2.8}$$

$$|\{i, w+l-i\}\cap A| = 1, \quad w+1 \leqslant i \leqslant l-1. \tag{2.9}$$

If $1 \leq i \leq w-1$ and $i \in A\setminus\{\frac{w}{2}\}$, then by (2.8), we have $w-i \notin A$. Moreover, $w+l-i > l$, thus, $w+l-i \notin A$.

If $w+1 \leq i \leq l-1$ and $i \in A\setminus\{\frac{w+l}{2}\}$, then by (2.9), we have $w+l-i \notin A$. Moreover, $w-i < 0$, thus, $w-i \notin A$.

In addition, for the trivial cases $i = 0$ or l, we have $S(w-i) = \{w, w+l\}$ or $\{w-l, w\}$, thus $|S(w-i)\cap A| = 0$.

Hence, if $i \in A\backslash\{\frac{w}{2}, \frac{w+l}{2}\}$, then $|S(w-i)\cap A| = 0$. Similarly, if $i \in [0,l]\backslash A$ or $i \in A\cap\{\frac{w}{2}, \frac{w+l}{2}\}$, then $|S(w-i)\cap A| = 1$.

This completes the proof of Lemma 2.2. □

Proof of Theorem 1.1. If $l \leq 2k-5$, then $W = \emptyset$. Now, we consider $2k-4 \leq l \leq 2k-3$. Assume that there exist distinct $w_1, w_2, w_3 \in W$ with $w_1 = \min(W)$ and $w_3 = \max(W)$. We now make a case distinction depending on the parity of w_1.

Case 1: $2 \mid w_1$.

Then $\frac{w_1}{2} < w_2 < w_3$. By Lemma 2.1, we have $\frac{w_1}{2} \in A$. Hence,

$$\frac{w_1}{2} \in A\setminus\left\{\frac{w_2}{2}, \frac{w_2+l}{2}\right\}, \frac{w_1}{2} \in A\setminus\left\{\frac{w_3}{2}, \frac{w_3+l}{2}\right\}.$$

By Lemma 2.2(1), we have $w_2 - \frac{w_1}{2}, w_3 - \frac{w_1}{2} \notin A$. Noting that $w_2, w_3 \in W$, by Lemma 2.2(2), we have

$$\left|S\left(w_3 - \left(w_2 - \frac{w_1}{2}\right)\right) \cap A\right| = 1, \left|S\left(w_2 - \left(w_3 - \frac{w_1}{2}\right)\right) \cap A\right| = 1. \tag{2.10}$$

Clearly, $w_3 - \left(w_2 - \frac{w_1}{2}\right) > 0$, so

$$w_3 - \left(w_2 - \frac{w_1}{2}\right) \in A. \tag{2.11}$$

If $w_3 - \left(w_2 - \frac{w_1}{2}\right) = \frac{w_1}{2}$, then $w_2 = w_3$, which is impossible.

If $w_3 - \left(w_2 - \frac{w_1}{2}\right) = \frac{w_1+l}{2}$, then $w_3 - w_2 = \frac{l}{2}$. Thus $l = 2k - 4$. By Lemma 2.1(1), we have $2 \mid w_2$ and $\frac{w_2}{2}, \frac{w_2+l}{2} \in A$. Hence

$$w_3 = \frac{w_2}{2} + \frac{w_2 + l}{2} \in 2^\wedge A,$$

which contradicts the assumption that $w_3 \in W$.

By (2.11) and the above discussion, we have

$$w_3 - \left(w_2 - \frac{w_1}{2}\right) \in A \setminus \left\{\frac{w_1}{2}, \frac{w_1 + l}{2}\right\}. \tag{2.12}$$

Noting that $w_1 \in W$ and

$$w_2 - \left(w_3 - \frac{w_1}{2}\right) = w_1 - \left(w_3 - \left(w_2 - \frac{w_1}{2}\right)\right),$$

by Lemma 2.2(1) and (2.12), we have

$$\left|S\left(w_2 - \left(w_3 - \frac{w_1}{2}\right)\right) \cap A\right| = 0,$$

which contradicts with (2.10).

Case 2: $2 \nmid w_1$.

By Lemma 2.1, we have $l = 2k - 3$. Let

$$\hat{A} = l - A = \{l - a : a \in A\}.$$

Then $\hat{A}$ is also a set of nonnegative integers that contains 0, l and $\gcd(\hat{A}) = 1$. Define $\hat{w} = l - w$ for any $w \in W$. If $S(\hat{w}) \cap 2^\wedge \hat{A} \neq \emptyset$, then there exist two distinct integers $\hat{a}, \hat{b} \in \hat{A}$ such that $\hat{w} = \hat{a} + \hat{b}$, that is, $l - w = l - a + l - b$, thus, $w + l = a + b$. Hence, $S(w) \cap 2^\wedge A \neq \emptyset$, a contradiction. So

$$S(\hat{w}) \cap 2^\wedge \hat{A} = \emptyset.$$

Write

$$\hat{W} = \{l - w : w \in W\}.$$

Then $|\hat{W}| = |W|$, $\min \hat{W} = l - w_3$, $\max \hat{W} = l - w_1$.

If $2 \nmid w_3$, then $\min \hat{W}$ is even. By Case 1, we know that this case is impossible.

If $2 \nmid w_1, 2 \mid w_2, 2 \mid w_3$, then by Lemma 2.1, $\frac{w_2}{2}, \frac{w_3}{2} \in A$. Noting that

$$\frac{w_2}{2} \in A \setminus \left\{\frac{w_1}{2}, \frac{w_1 + l}{2}\right\}, \quad \frac{w_2}{2} \in A \setminus \left\{\frac{w_3}{2}, \frac{w_3 + l}{2}\right\},$$

by Lemma 2.2(1), we have

$$\left|S\left(w_1-\frac{w_2}{2}\right)\cap A\right|=0 \text{ and } \left|S\left(w_3-\frac{w_2}{2}\right)\cap A\right|=0, \tag{2.13}$$

thus, $\frac{w_2}{2}\neq w_1$. We divide into the following two cases:

SUBCASE 2.1: If $\frac{w_2}{2}<w_1$, then $w_1-\frac{w_2}{2}>0$, thus by (2.13) and Lemma 2.2(2), we have

$$\left|S\left(w_3-\left(w_1-\frac{w_2}{2}\right)\right)\cap A\right|=1 \text{ and } \left|S\left(w_1-\left(w_3-\frac{w_2}{2}\right)\right)\cap A\right|=1.$$

Clearly, $w_3-\left(w_1-\frac{w_2}{2}\right)>0$, thus $w_3-\left(w_1-\frac{w_2}{2}\right)\in A$. It is easy to see that

$$S(w_2)=w_3-\left(w_1-\frac{w_2}{2}\right)+S\left(w_1-\left(w_3-\frac{w_2}{2}\right)\right)$$

and

$$w_3-\left(w_1-\frac{w_2}{2}\right)\notin S\left(w_1-\left(w_3-\frac{w_2}{2}\right)\right),$$

thus,

$$S(w_2)\cap 2^\wedge A\neq\emptyset,$$

which contradicts the assumption that $w_2\in W$.

SUBCASE 2.2: If $\frac{w_2}{2}>w_1$, then $w_1+l-\frac{w_2}{2}>0$. Since $w_3-\frac{w_2}{2}>\frac{w_3}{2}>\frac{w_2}{2}>w_1$, by (2.13) and Lemma 2.2(2), we have

$$\left|S\left(w_1-\left(w_3-\frac{w_2}{2}\right)\right)\cap A\right|=1 \text{ and } \left|S\left(w_3-\left(w_1+l-\frac{w_2}{2}\right)\right)\cap A\right|=1.$$

Since $w_1-\left(w_3-\frac{w_2}{2}\right)<0$, we have $w_1+l-\left(w_3-\frac{w_2}{2}\right)\in A$. It is easy to see that

$$S(w_2)=w_1+l-\left(w_3-\frac{w_2}{2}\right)+S\left(w_3-\left(w_1+l-\frac{w_2}{2}\right)\right)$$

and

$$w_1+l-\left(w_3-\frac{w_2}{2}\right)\notin S\left(w_3-\left(w_1+l-\frac{w_2}{2}\right)\right),$$

thus,

$$S(w_2)\cap 2^\wedge A\neq\emptyset,$$

which contradicts the assumption that $w_2\in W$.

If $2\nmid w_1, 2\nmid w_2, 2\mid w_3$, then by Lemma 2.1, $l=2k-3$. Thus, $2\nmid\min\hat{W}, 2\mid\hat{w}_2, 2\mid\max\hat{W}$. This case as same as the above case, it is also impossible.

In all, we have $|W|\leqslant 2$.

This completes the proof of Theorem 1.1. □

3. Proof of Propositions 1.2, 1.3 and 1.4

Lemma 3.1. *Let A be a set of $k > 7$ integers such that $A \subseteq [0, l]$, $0, l \in A$ and $l \leqslant 2k - 3$. If $W = \{w_1, w_2\}$ with $\gcd(w_2 - w_1, l) = m$, then* $\frac{l}{m} \equiv 1 \pmod 2$.

Proof. Obviously, if $l = 2k - 3$, then m is odd, so $\frac{l}{m} \equiv 1 \pmod 2$. Now we assume that $l = 2k - 4$ and $w_1 < w_2$. By Lemma 2.1(1), we have $2 \mid w_1, 2 \mid w_2$, so $m \geqslant 2$. If $\frac{l}{m} \equiv 0 \pmod 2$, then

$$\frac{w_2}{2} \equiv \frac{w_2 + l}{2} \pmod{m}, \quad \frac{w_2 - w_1}{m} \equiv 1 \pmod{2}. \tag{3.1}$$

Thus $\frac{w_2 - w_1}{2m} \notin \mathbb{Z}, \frac{l}{2m} \in \mathbb{Z}$.

For any integer $x \in \left[0, \frac{l}{2m}\right]$, write

$$r(x) = \frac{w_1}{2} + x(w_2 - w_1) - q(x)l, \tag{3.2}$$

where $q(x)$ is the unique integer such that $r(x) \in [0, l)$.

Next, we shall show that if $r(x) \in A$ for some $x \in [1, \frac{l}{2m}]$, then $r(x - 1) \in A$.

By $\gcd(w_2 - w_1, l) = m$ and (3.2), we have

$$r(x) \equiv \frac{w_1}{2} \pmod{m}.$$

Moreover, by (3.1) we have $\frac{w_2}{2} \not\equiv \frac{w_1}{2} \pmod{m}$. If $r(x) \in A$, then

$$r(x) \in A \setminus \left\{ \frac{w_2}{2}, \frac{w_2 + l}{2} \right\}. \tag{3.3}$$

If $r(x) < w_2$, then by (3.3) and Lemma 2.2(1), we have $w_2 - r(x) \notin A$. Noting that $w_1 \in W$, by Lemma 2.2(2), we have

$$|S(w_1 - (w_2 - r(x))) \cap A| = 1.$$

By (3.2) we have

$$w_1 - (w_2 - r(x)) = \frac{w_1}{2} + (x - 1)(w_2 - w_1) - q(x)l. \tag{3.4}$$

If $w_1 - (w_2 - r(x)) \in A$, then $w_1 - (w_2 - r(x)) \in [0, l)$. Thus, $q(x - 1) = q(x)$. By (3.2) and (3.4), we have

$$r(x - 1) = w_1 - (w_2 - r(x)) \in A.$$

If $w_1 - (w_2 - r(x)) + l \in A$, then $w_1 - (w_2 - r(x)) + l \in [0, l)$. Thus, $q(x - 1) = q(x) - 1$. By (3.2) and (3.4), we have

$$r(x - 1) = w_1 - (w_2 - r(x)) + l \in A.$$

If $r(x) > w_2$, then by (3.3) and Lemma 2.2, we have $w_2 + l - r(x) \notin A$ and

$$|S(w_1 - (w_2 + l - r(x))) \cap A| = 1.$$

Similar to the above discussion, we also have $r(x-1) \in A$. Moreover, since we can write

$$\frac{w_1+l}{2} = \frac{w_1}{2} + \frac{l}{2m}(w_2-w_1) - \left(\frac{w_2-w_1}{2m} - \frac{1}{2}\right) l,$$

we have $r\left(\frac{l}{2m}\right) \in A$. Hence, $r(x) \in A$ for all $x \in \left[0, \frac{l}{2m}\right]$. So

$$r(0) = \frac{w_1}{2} \in A, \quad r(1) = \frac{w_1}{2} + (w_2 - w_1) \in A,$$

therefore, $w_2 = r(0) + r(1) \in 2^\wedge A$, which contradicts the assumption that $w_2 \in W$.

Hence $\frac{l}{m} \equiv 1 \pmod 2$.

This completes the proof of Lemma 3.1. □

Remark 3.2*:* Let the notations be as in Lemma 3.1. Noting that if $\frac{w_2-w_1}{m}$ is even, then

$$\frac{w_1}{2} = \frac{w_2}{2} + \left(\frac{l}{2m} - \frac{1}{2}\right)(w_2-w_1) - \frac{w_2-w_1}{2m} l, \tag{3.5}$$

$$\frac{w_1+l}{2} = \frac{w_2+l}{2} + \left(\frac{l}{2m} - \frac{1}{2}\right)(w_2-w_1) - \frac{w_2-w_1}{2m} l. \tag{3.6}$$

If $\frac{w_2-w_1}{m}$ is odd, then

$$\frac{w_1+l}{2} = \frac{w_2}{2} + \left(\frac{l}{2m} - \frac{1}{2}\right)(w_2-w_1) - \left(\frac{w_2-w_1}{2m} - \frac{1}{2}\right) l, \tag{3.7}$$

$$\frac{w_1}{2} = \frac{w_2+l}{2} + \left(\frac{l}{2m} - \frac{1}{2}\right)(w_2-w_1) - \left(\frac{w_2-w_1}{2m} + \frac{1}{2}\right) l. \tag{3.8}$$

By the above (3.5)–(3.8), we know that $\frac{w_1}{2}$ and $\frac{w_1+l}{2}$ can be represented as the form $r(x)$ defined in (3.2). These equations will be used later.

Proof of Proposition 1.2. For any two integers $x_1, x_2 \in [0, \frac{l}{m}-1]$, if $r_v(x_1) = r_v(x_2)$, then we have

$$(x_1-x_2)(w_2-w_1) = (q(x_1)-q(x_2))l,$$

noting that $(\frac{w_2-w_1}{m}, \frac{l}{m}) = 1$, we have

$$\frac{l}{m} \mid (x_1 - x_2),$$

thus $x_1 = x_2$. Hence

$$|\mathcal{D}^-(v) \cup \mathcal{D}^+(v)| = \frac{l}{m}, \tag{3.9}$$

$$\mathcal{D}^-(v) \cap \mathcal{D}^+(v) = \emptyset. \tag{3.10}$$

(1) We begin by proving that $\mathcal{D}^-(v) \subseteq A$. By Lemma 2.1, we have $v = r_v(0) \in V \subseteq A$. By (3.9), we have $r_v(x) \neq v$ for all $x \in [1, \frac{l}{2m} - \frac{1}{2}]$. By

Lemma 3.1, we have $\frac{w_2}{2} \not\equiv \frac{w_2+l}{2} \pmod{m}$. Since $r_v(x) \equiv v \pmod{m}$ and $v \in \left\{\frac{w_2}{2}, \frac{w_2+l}{2}\right\}$, we have

$$r_v(x) \notin \left\{\frac{w_2}{2}, \frac{w_2+l}{2}\right\}$$

for all $x \in [1, \frac{l}{2m} - \frac{1}{2}]$. By the analogous discussion of Lemma 3.1, we have if $r_v(x) \in A \backslash \left\{\frac{w_2}{2}, \frac{w_2+l}{2}\right\}$ for some $x \in [1, \frac{l}{2m} - \frac{1}{2}]$, then $r_v(x-1) \in A$. By (3.5)–(3.8), we have

$$r_v\left(\frac{l}{2m} - \frac{1}{2}\right) = \frac{w_1}{2} \text{ or } \frac{w_1+l}{2},$$

thus,

$$r_v\left(\frac{l}{2m} - \frac{1}{2}\right) \in A \backslash \left\{\frac{w_2}{2}, \frac{w_2+l}{2}\right\}.$$

Hence, $r_v(x) \in A$ for all $x \in \left[0, \frac{l}{2m} - \frac{1}{2}\right]$. So $\mathcal{D}^-(v) \subseteq A$.

(2) We now prove that $\mathcal{D}^+(v) \cap A$ is empty. For any $r_v(x) \in \mathcal{D}^-(v)$ with $x \neq \frac{l}{2m} - \frac{1}{2}$, we have

$$v - l < q(x)l - x(w_2 - w_1) \leqslant v,$$

thus

$$\begin{aligned} & v + \left(\frac{l}{m} - 1 - x\right)(w_2 - w_1) - \left(\frac{w_2 - w_1}{m} - q(x)\right) l \\ = \;& v + (q(x)l - x(w_2 - w_1)) - (w_2 - w_1) \\ \in \;& (2v - l - (w_2 - w_1), 2v - (w_2 - w_1)]. \end{aligned}$$

Since $v \in \{\frac{w_2}{2}, \frac{w_2+l}{2}\}$, we have

$$\begin{aligned} & v + \left(\frac{l}{m} - 1 - x\right)(w_2 - w_1) \\ & - \left(\frac{w_2 - w_1}{m} - q(x)\right) l \in (w_1 - l, l + w_1]. \end{aligned} \tag{3.11}$$

It is clear that

$$\frac{l}{2m} + \frac{1}{2} \leqslant \frac{l}{m} - 1 - x \leqslant \frac{l}{m} - 1. \tag{3.12}$$

By (3.11) and (3.12), there exists an integer $i \in \{-1, 0, 1\}$ such that

$$\begin{aligned} r_v\left(\frac{l}{m} - 1 - x\right) \;:=\;& v + \left(\frac{l}{m} - 1 - x\right)(w_2 - w_1) \\ & - \left(\frac{w_2 - w_1}{m} - i - q(x)\right) l \in \mathcal{D}^+(v). \end{aligned}$$

By (3.10), we have

$$r_v\left(\frac{l}{m} - 1 - x\right) \neq r_v(x).$$

If $r_v\left(\frac{l}{m}-1-x\right)\in A$, then $r_v\left(\frac{l}{m}-1-x\right)\in[0,l]$, thus,

$$r_v(x)+r_v\left(\frac{l}{m}-1-x\right)=2v-(w_2-w_1)+il\in[0,2l].$$

Hence

$$r_v(x)+r_v\left(\frac{l}{m}-1-x\right)=w_1 \text{ or } w_1+l,$$

it implies that w_1 or $w_1+l\in 2^\wedge A$, which is contradicts with $w_1\in W$. So $\mathcal{D}^+(v)\cap A=\emptyset$.

(3) Finally, we prove that $0\in\mathcal{D}^-(v)$ if $v\equiv 0 \pmod m$ for some $v\in V$. Let $v\equiv 0 \pmod m$. Then by (3.9) and (3.10), we have

$$\mathcal{D}^-(v)\cup\mathcal{D}^+(v)=m\mathbb{Z}\cap[0,l).$$

Assume that $0\notin\mathcal{D}^-(v)$, so $0\in\mathcal{D}^+(v)$. By Lemma 3.1, we have $\frac{l}{m}\equiv 1 \pmod 2$, so $\frac{l}{m}\geqslant 3$. As $0\in\mathcal{D}^+(v)$, there exist an integer $x_0\in[\frac{l}{2m}+\frac{1}{2},\frac{l}{m}-1]$ and an integer $q(x_0)$ such that

$$v+x_0(w_2-w_1)-q(x_0)l=0,$$

thus

$$v+\left(\frac{l}{m}-x_0\right)(w_2-w_1)-\left(\frac{w_2-w_1}{m}-q(x_0)\right)l=2v.$$

Hence, there exists $i\in\{0,1\}$ such that

$$v+\left(\frac{l}{m}-x_0-1\right)(w_2-w_1)-\left(\frac{w_2-w_1}{m}-q(x_0)+i\right)l=w_1.$$

Since

$$0\leqslant\frac{l}{m}-x_0-1\leqslant\frac{l}{2m}-\frac{3}{2},$$

we must have $w_1\in\mathcal{D}^-(v)$, so by (1), we have $w_1\in A$, a contradiction.

This completes the proof of Proposition 1.2. □

Remark 3.3*:* By Proposition 1.2, we actually obtain $(\frac{l}{2m}+\frac{1}{2})|V|$ integers of A. In particular, if $m=1$, then $l=2k-3$ and

$$A=\mathcal{D}^-(v)\cup\{l\},$$

where $v=\frac{w}{2}$ or $\frac{w+l}{2}$.

Proof of Proposition 1.3. Since $u\in A\setminus\left\{\frac{w_2}{2},\frac{w_2+l}{2}\right\}$, by Lemma 2.2(1), we have $w_2-u\notin A$. By Lemma 2.2(2), we have

$$|S(w_1-(w_2-u))\cap A|=1.$$

Moreover, $w_1-(w_2-u)=u-(w_2-w_1)<0$, thus $w_1-(w_2-u)+l\in A$. Noting that

$$u+r\left(\frac{l}{m}-1\right)=u+l-(w_2-w_1)=w_1-(w_2-u)+l,$$

we have $u+r\left(\frac{l}{m}-1\right)\in A$.

Similar to the proof of Lemma 3.1, we can show that if $u + r\,(x) \in A$ for some $x \in \left[1, \frac{l}{m} - 1\right]$, then $u + r(x-1) \in A$. Hence, $u + H \subseteq A$.

This completes the proof of Proposition 1.3. $\square$

Proof of Proposition 1.4. Let H be as in Proposition 1.3. Then $H = m\mathbb{Z} \cap [0, l)$. By Proposition 1.2(1) and Proposition 1.3, we have

$$\{l\} \cup (U + H) \cup \bigcup_{v \in V} \mathcal{D}^-(v) \subseteq A.$$

Conversely, let $a \in A$ be an integer with $a \neq l$ and $a \notin \bigcup_{v \in V} \mathcal{D}^-(v)$. By Proposition 1.2(2), we have $a \notin \bigcup_{v \in V} \mathcal{D}^+(v)$. If $a \equiv v \pmod m$ for some $v \in V$, then there exist an integer $x \in [0, \frac{l}{m} - 1]$ and an integer $q(x)$ such that

$$a = v + x(w_2 - w_1) - q(x)l,$$

a contradiction. Thus, $a \not\equiv v \pmod m$ for any $v \in V$.

Let $u' \in [0, m-1]$ be an integer such that $u' \equiv a \pmod m$. Then there exists an integer $x_0 \in [0, \frac{l}{m} - 1]$ such that $a = u' + r(x_0)$, where $r(x_0) \in H$. If $a \notin U + H$, then $u' \in [0, m-1] \backslash A$. Similar to the proof Lemma 3.1, we can show that if $u' + r\,(x) \in A$ for some $x \leqslant x_0$, then $u' + r(x-1) \in A$. Thus, $u' \in A$, which is impossible. Hence $a \in U + H$.

So,

$$A = \{l\} \cup (U + H) \cup \bigcup_{v \in V} \mathcal{D}^-(v).$$

This completes the proof of Proposition 1.4. $\square$

Remark 3.4*:* Let the notations be as in Proposition 1.4. Then

(1) $|U| = \left\lceil \frac{m-2}{2} \right\rceil$;

(2) If $u \in [0, m-1] \backslash A$ and $2u \not\equiv w_2 \pmod m$, then $(u + H) \cap A = \emptyset$.

4. Proof of Theorem 1.5

Let $A = \{0 = a_0 < \cdots < a_{k-1} = l\}$ and $l = 2k - 4$ or $2k - 3$. Consider the set

$$T = \{a_i : 1 \leqslant i \leqslant k-1\} \dot\cup \{a_i + l : 1 \leqslant i \leqslant k-2\}.$$

Then $T \subseteq 2^\wedge A$ and $|T| = 2k - 3$. Let $B = [0, l] \backslash A$. Then we have $|B| = l + 1 - k$. By Theorem 1.1, we have $|W| \leqslant 2$ and

$$|S(w) \cap 2^\wedge A| \geqslant 1$$

for each $w \in B \backslash W$. Since $B \backslash W \subseteq [0, l]$ and $B \cap A = \emptyset$, we have $T \cap (B \backslash W) = \emptyset$. Hence

$$|2^\wedge A| \geqslant |T| + |B \backslash W|.$$

If $l = 2k - 3$, then

$$\begin{aligned} |2^\wedge A| &\geqslant |T| + |B| - 2 \\ &= (2k-3) + (l + 1 - k) - 2 \\ &= 3k - 7. \end{aligned}$$

If $l = 2k-4$ and $|W| \leqslant 1$, then

$$\begin{aligned} |2^\wedge A| &\geqslant |T| + |B| - 1 \\ &= (2k-3) + (l+1-k) - 1 \\ &= 3k-7. \end{aligned}$$

Now, we consider that $l = 2k-4$ and $|W| = 2$. Let $W = \{w_1, w_2\}$ with $\gcd(w_2 - w_1, l) = m$. By Lemma 2.1(1), we have w_1 and w_2 are both even, thus $m \geqslant 2$. By Lemma 3.1, we have $\frac{l}{m}$ is odd, thus, $\frac{l}{m} \geqslant 3$. By Proposition 1.4, we have

$$A = \{l\} \cup (U + H) \cup \bigcup_{v \in V} \mathcal{D}^-(v),$$

where $V = \left\{\frac{w_2}{2}, \frac{w_2+l}{2}\right\}$, $H = m\mathbb{Z} \cap [0, l)$ and U is defined as in Proposition 1.4.

We will show that there exists an integer $w \in [0, l] \backslash A$ such that

$$\left|S(w) \cap 2^\wedge A\right| = 2.$$

Case 1: $v \not\equiv 0 \pmod m$ for all $v \in V$.

Then by Proposition 1.4, we have $0 \in U$. By Proposition 1.3, we have

$$m\mathbb{Z} \cap [0, l) = 0 + H \subseteq A.$$

By Lemma 3.1, we have $\frac{l}{m} \equiv 1 \pmod 2$, thus $2(w_2 - w_1) \neq l$. Now we divide into the following three cases:

Subcase 1.1: $2(w_2 - w_1) < l$.

By the definitions of $\mathcal{D}^-(v)$ and $\mathcal{D}^+(v)$ of Proposition 1.2 and (3.5)–(3.8), we have $\frac{w_1}{2} + (w_2 - w_1) \in \mathcal{D}^+(v)$, thus,

$$\frac{w_1}{2} + (w_2 - w_1) \notin A.$$

If $\frac{w_1}{2} = w_2 - w_1$, then again by (3.5)–(3.8), we have $v \equiv 0 \pmod m$, giving a contradiction. Hence $\frac{w_1}{2} \neq w_2 - w_1$. Since $w_1 \notin A$, by Lemma 2.2(2), we have $|S(w_2 - w_1) \cap A| = 1$, thus, $w_2 - w_1 \in A$. Also, $\frac{w_1}{2} \in A$, we have

$$\frac{w_1}{2} + (w_2 - w_1) \in 2^\wedge A. \tag{4.1}$$

Let

$$\delta = \left\lfloor \frac{\frac{w_1}{2}}{w_2 - w_1} \right\rfloor.$$

By (3.5) and (3.8), we have

$$0 \leqslant \delta \leqslant \frac{l}{2m} - \frac{1}{2} + \frac{w_2}{2(w_2 - w_1)} - \frac{l}{2m}.$$

Since $m \leqslant w_2 - w_1$ and $w_2 < l$, we have

$$0 \leqslant \delta < \frac{l}{2m} - \frac{1}{2}.$$

It is clear that $2\delta(w_2-w_1)\leqslant w_1<l$, thus,

$$(2\delta+1)(w_2-w_1)\leqslant w_2<l.$$

Hence,

$$c(w_2-w_1)\in m\mathbb{Z}\cap[0,l]\subseteq A$$

for any $c\in[0,\max\{2\delta+1,2\}]$. Since $\delta+2\leqslant\max\{2\delta+1,2\}$, we have

$$(\delta+2)(w_2-w_1)\in A.$$

Since

$$\delta=\left\lfloor\frac{\frac{w_1}{2}}{w_2-w_1}\right\rfloor,$$

we have $(\delta+1)(w_2-w_1)>\frac{w_1}{2}$, thus,

$$\frac{w_1}{2}-(\delta+1)(w_2-w_1)+l\in[0,l].$$

By (3.5) and (3.8), we have

$$\frac{w_1}{2}-(\delta+1)(w_2-w_1)+l=r_v\left(\frac{l}{2m}-\frac{1}{2}-(\delta+1)\right)\in\mathcal{D}^-(v)\subseteq A.$$

Since $v\not\equiv 0\pmod m$, we have $r_v\left(\frac{l}{2m}-\frac{1}{2}-(\delta+1)\right)\not\equiv 0\pmod m$, thus,

$$\left(\frac{w_1}{2}-(\delta+1)(w_2-w_1)+l\right)\neq(\delta+2)(w_2-w_1).$$

Hence

$$\frac{w_1}{2}+(w_2-w_1)+l=\left(\frac{w_1}{2}-(\delta+1)(w_2-w_1)+l\right)+(\delta+2)(w_2-w_1)\in 2^\wedge A. \tag{4.2}$$

By (4.1) and (4.2), we have

$$\left|S\left(\frac{w_1}{2}+(w_2-w_1)\right)\cap 2^\wedge A\right|=2.$$

Subcase 1.2: $2(w_2-w_1)>l$ and $l-2m\geqslant w_2-w_1$.

Then $l<2(w_2-w_1)\leqslant 2(l-2m)$, thus $l>4m$. Hence $\frac{l}{m}\geqslant 5$. By Proposition 1.4, we have

$$cm,l+cm-(w_2-w_1)\in m\mathbb{Z}\cap[0,l]\subseteq A,\quad\forall\,1\leqslant c\leqslant\frac{w_2-w_1}{m}-1. \tag{4.3}$$

We have the following inequality

$$\begin{aligned}\left(\frac{l}{2m}-\frac{1}{2}\right)(w_2-w_1)&=\frac{(w_2-w_1)}{2m}l-\frac{1}{2}(w_2-w_1)\\ &\leqslant\frac{l-2m}{2m}l-\frac{1}{2}(w_2-w_1)<\left(\frac{l}{2m}-\frac{1}{2}-1\right)l+\frac{w_1+l}{2}.\end{aligned}$$

Let x be the smallest integer with $x\in\left[2,\frac{l}{2m}-\frac{1}{2}\right]$ such that

$$x(w_2-w_1)<(x-1)l+\frac{w_1+l}{2}.$$

Write

$$\lambda_1 := \frac{w_1 + l}{2} - x(w_2 - w_1) + (x-1)l,$$

$$\lambda_2 := \frac{w_1 + l}{2} - (x-1)(w_2 - w_1) + (x-1)l.$$

Then by (3.6) and (3.7), we have

$$\lambda_1 = r_v\left(\frac{l}{2m} - \frac{1}{2} - x\right), \quad \lambda_2 = r_v\left(\frac{l}{2m} - \frac{1}{2} - (x-1)\right).$$

By Proposition 1.2(1), we have $\lambda_1, \lambda_2 \in \mathcal{D}^-(v) \subseteq A$.

Noting that

$$|\mathcal{D}^-(v)\backslash\{\lambda_1\}| = \frac{l}{2m} - \frac{3}{2} < \frac{w_2 - w_1}{m} - \frac{3}{2},$$

there exists an integer $1 \leqslant c_0 \leqslant \frac{w_2 - w_1}{m} - 1$ such that $\lambda_1 + c_0 m \notin \mathcal{D}^-(v)$, thus,

$$\lambda_1 + c_0 m \notin A.$$

Since $v \not\equiv 0 \pmod{m}$, we have $\lambda_1 \not\equiv 0 \pmod{m}$, thus, $\lambda_1 \neq c_0 m$. By (4.3), we have

$$\lambda_1 + c_0 m \in 2^\wedge A.$$

Similarly, we have

$$\lambda_1 + c_0 m + l = \lambda_2 + l + c_0 m - (w_2 - w_1) \in 2^\wedge A.$$

Therefore

$$\left|S\left(\lambda_1 + c_0 m\right) \cap 2^\wedge A\right| = 2.$$

Subcase 1.3: $2(w_2 - w_1) > l$ and $l - m = w_2 - w_1$.

For any integer $0 \leqslant c \leqslant \frac{l}{2m} - \frac{1}{2}$, we have $\frac{w_2}{2} - cm$ and $\frac{w_2 + l}{2} - cm$ are all greater than zero. By Proposition 1.2(1), we have

$$\frac{w_2}{2} - cm, \frac{w_2 + l}{2} - cm \in A, \quad \forall\ 0 \leqslant c \leqslant \frac{l}{2m} - \frac{1}{2},$$

that is,

$$\left\{\frac{w_1}{2}, \frac{w_1}{2} + m, \ldots, \frac{w_2}{2}, \frac{w_2 + m}{2}, \frac{w_2 + m}{2} + m, \ldots, \frac{w_2 + l}{2}\right\} \subseteq A.$$

thus,

$$w_1 + m \in 2^\wedge A, \quad w_2 + 2m = w_1 + m + l \in 2^\wedge A.$$

Hence

$$\left|S\left(w_1 + m\right) \cap 2^\wedge A\right| = 2.$$

In addition, by Remark 3.4(2), we have $w_1 + m \notin A$.

Case 2: $v \equiv 0 \pmod m$ for some $v \in V$.

Then $w_1 \equiv w_2 \equiv 0 \pmod m$. Thus, $l - m > w_2 - w_1$, it implies that

$$\frac{l}{2m} - \frac{1}{2} > \frac{w_2 - w_1}{2m}.$$

By (3.5)–(3.8), there exists an integer $x \in [0, \frac{l}{2m} - \frac{1}{2})$ such that

$$r_v(x+1) = r_v(x) + (w_2 - w_1).$$

In this part, we assume that $V = \{v_1, v_2\}$ such that $v_1 \equiv 0 \pmod m$, so

$$v_2 \equiv \frac{m}{2} \pmod m.$$

By Proposition 1.2(3), we have $0 \in \mathcal{D}^-(v)$, thus, there exists an integer $0 < x_0 < \frac{l}{2m} - \frac{1}{2}$ such that

$$r_{v_1}(x_0) := v_1 + x_0(w_2 - w_1) - q(x_0)l = 0. \tag{4.4}$$

Moreover, by the definition of $\mathcal{D}^-(v)$ of Proposition 1.2, we have

$$r_{v_1}(x_0 - c) = r_{v_1}(x_0) - c(w_2 - w_1) + l = l - c(w_2 - w_1) \in A \tag{4.5}$$

for any $c \in [1, \min\{\lfloor \frac{l}{w_2 - w_1} \rfloor, x_0\}]$.

Subcase 2.1: $m \geqslant 4$.

By Remark 3.4(1), we have $U \neq \emptyset$. By the definition of U of Proposition 1.4, we have one of $\frac{m}{4}$ and $\frac{3m}{4}$ belong to U. Without loss of generality, we assume that $\frac{m}{4} \in U$, so $\frac{3m}{4} \notin U$. By Proposition 1.4, we have

$$\frac{m}{4} + H \subseteq A, \quad \left(\frac{3m}{4} + H\right) \cap A = \emptyset,$$

thus,

$$\frac{m}{4} \in A, \quad \frac{m}{4} + l - (w_2 - w_1) \in A.$$

Since $\frac{m}{4} + v_2 \equiv \frac{3m}{4} \pmod m$, we have

$$\left(\frac{m}{4} + H + \mathcal{D}^-(v_2)\right) \cap A = \emptyset.$$

Based on the previous discussion, there exists an integer $x \in [0, \frac{l}{2m} - \frac{1}{2})$ such that

$$r_{v_2}(x+1) = r_{v_2}(x) + (w_2 - w_1).$$

Hence

$$\frac{m}{4} + r_{v_2}(x) \in 2^\wedge A$$

and

$$\frac{m}{4} + r_{v_2}(x) + l = \left(\frac{m}{4} + l - (w_2 - w_1)\right) + r_{v_2}(x+1) \in 2^\wedge A,$$

so

$$\left| S\left(\frac{m}{4} + r_{v_2}(x)\right) \cap 2^\wedge A \right| = 2.$$

SUBCASE 2.2: By Lemma 2.1, we have $l = 2k - 4$ and w_1, w_2 are even, thus, m is even, so we only need consider $m = 2$. If $m = 2$, then $U = \emptyset$. By Proposition 1.4, we have

$$A = \{l\} \cup \bigcup_{v \in V} \mathcal{D}^-(v).$$

By the definition of $\mathcal{D}^-(v)$ of Proposition 1.2, one of the following three conditions holds:
(1) $\frac{w_2}{2}, \frac{w_2}{2} + (w_2 - w_1), \frac{w_2+l}{2}, \frac{w_2+l}{2} + (w_2 - w_1) \in A$;
(2) $\frac{w_2}{2}, \frac{w_2}{2} + (w_2 - w_1) - l, \frac{w_2+l}{2}, \frac{w_2+l}{2} + (w_2 - w_1) - l \in A$;
(3) $\frac{w_2}{2}, \frac{w_2}{2} + (w_2 - w_1), \frac{w_2+l}{2}, \frac{w_2+l}{2} + (w_2 - w_1) - l \in A$.
We assume that (1) holds. It implies that

$$|S(2w_2 - w_1) \cap 2^\wedge A| = 2.$$

Now we prove that $2w_2 - w_1 \notin A$. First, Condition (1) implies that

$$\frac{w_2}{2} + (w_2 - w_1) < l, \quad \frac{w_2 + l}{2} + (w_2 - w_1) < l.$$

By (4.4), we have $x > 1$ and $l > 2(w_2 - w_1)$, and by (4.5), we have

$$l - 2(w_2 - w_1) \in A.$$

If $2w_2 - w_1 = \frac{w_2}{2} + \frac{w_2}{2} + (w_2 - w_1) = l - (w_2 - w_1)$, then

$$w_2 = l - 2(w_2 - w_1) \in A,$$

which is impossible. Hence

$$2w_2 - w_1 \neq l - (w_2 - w_1).$$

If $2w_2 - w_1 \in A$, then

$$2w_2 - w_1 + l - (w_2 - w_1) = w_2 + l \in 2^\wedge A,$$

which is impossible. Hence, $2w_2 - w_1 \notin A$.
If (2) holds, then the proof is similar to (1), we omit it.
If (3) holds, then

$$\left| S\left(2w_2 - w_1 - \frac{l}{2}\right) \cap 2^\wedge A \right| = 2.$$

Now we prove that $2w_2 - w_1 - \frac{l}{2} \notin A$. If not, then $2w_2 - w_1 - \frac{l}{2} \in \mathcal{D}^-(v_2)$, thus, there exists a positive integer y such that

$$r_{v_2}(y) = 2w_2 - w_1 - \frac{l}{2} \in A,$$

it follows that,

$$v_1 + (1 - y)(w_2 - w_1) - (1 - q(y))l = 0.$$

By (4.4), we have $r_{v_1}(x_0) = 0$, thus,

$$r_{v_1}(x_0) = v_1 + (1 - y)(w_2 - w_1) - (1 - q(y))l.$$

Hence

$$(x_0 + y - 1)(w_2 - w_1) = (q(x_0) + q(y) - 1)l,$$

so

$$(x_0 + y - 1)\frac{(w_2 - w_1)}{2} = (q(x_0) + q(y) - 1)\frac{l}{2}.$$

Since $\gcd(w_2 - w_1, l) = 2$, we have $\gcd(\frac{w_2-w_1}{2}, \frac{l}{2}) = 1$, thus,

$$\frac{l}{2} | x_0 + y - 1.$$

Since $x_0, y \in [1, \frac{l}{4} - \frac{1}{2}]$, we have

$$0 < x_0 + y - 1 < \frac{l}{2},$$

giving a contradiction. Hence, $2w_2 - w_1 - \frac{l}{2} \notin A$.

In all, we have

$$|2^\wedge A| \geqslant |T| + |B \backslash W| \geqslant 3k - 7.$$

This completes the proof of Theorem 1.5.

Acknowledgment

The authors would like to thank the referee for helpful comments and valuable suggestions.

References

[1] J. Bourgain, *On triples in arithmetic progression*, Geom, Funct. Anal. **9**(1999), 968–984.

[2] G. A. Freiman, *The addition of finite sets*, I, Izv. Vysš. Učebn. Zaved. Matematika **13**(1959), 202–213.

[3] G. A. Freiman, L. Low and J. Pitman, *Sumsets with distinct summands and the conjecture of Erdős-Heilbronn on sums residues*, Asterisque, **258**(1999), 163–172.

[4] V. F. Lev, *Restricted set addition in groups, I. The classical setting*, J. London Math. Soc. **62**(2000), 27–40.

[5] M. B. Nathanson, *Additive number theory. Inverse problems and the geometry of sumsets*, Graduate Texts in Math. 165, Springer-Verlag, New York, 1996.

[6] I. Z. Ruzsa, *Arithmetical progressions and the number of sums*, Period. M. Hung. **25**(1992), 105–111.

[7] T. Schoen, *The cardinality of restricted sumsets*, J. Number Theory **96**(2002), 48–54.

[8] M. Tang and W. H. Wang, *Some remarks on sumsets and restricted sumsets*, Bull. Korean Math. Soc. **56**(2019), 667–673.

[9] ______, *Some remarks on a conjecture of Freiman and Lev*, Adv. Math. (China), to appear.

School of Mathematics and Statistics, Anhui Normal University, Wuhu 241002, P. R. China
E-mail address: wangyujie9291@126.com

School of Mathematics and Statistics, Anhui Normal University, Wuhu 241002, P. R. China
E-mail address: tmzzz2000@163.com