Original Research Article

Densification of Witnesses for Randomized Algorithm Design

Abstract

We investigate the densification of witnesses for randomized algorithm design and its application in factoring integers. By defining a set operation named with Cartesian subtraction on countable finite sets and proving its properties, we show that the Cartesian subtraction can densify certain elements in a countable set so as to promote abundance of witnesses for the randomized algorithm design. We also prove that the Cartesian subtraction of two sets containing consecutive integers can form a triangular lattice zone that has a higher density of witnesses. Through designing an algorithm of a two dimensional simple random walk on the triangular lattice zone, we demonstrate that composite integers can be factored by means of the random walk. Our approach and experience indicate that the Cartesian subtraction is feasible and workable to densify the small witnesses in a countable finite set.

Keywords: Set operation; randomized algorithm; random walk; integer factorization

2010 Mathematics Subject Classification:03E99,68Q87, 68W20, 60G50

1 Introduction

Finding out a hidden (or unknown) objective element in a set is a necessary task in many scientific research activities, e.g., solving an equation. When we want to find an unknown object related to an element in a discrete set, e.g., find a divisor of a composite integer N, randomized algorithms are frequently applied, as claimed in [1] and summarized in [2]. When applying the random algorithm, the abundance of witnesses is a critical issue to affect the searching cost, as Richard M Karp pointed out [3]. Promoting the efficiency to find a witness is sure to reduce the searching cost. Accordingly, scholars made certain researches on the topic. Some researched the witness generators [4][5][6], and some researched efficient searching techniques in terms of small witnesses[7][8][9]. However, seen in the literatures, few have been found to concentrate witnesses or make witnesses denser. Densification of witnesses is sure to increase the probability of successful searches and reduce the searching cost.

In this paper, we aim at densification of the witnesses and its application in integer factorization. By defining a Cartesian subtraction on countable finite sets, we discover that certain single element in a countable finite set can be made repeated finite many times and distributed sparsely in the resulted set formed by the Cartesian subtraction. By such means, the abundance of witnesses is naturally

promoted for designing the randomized algorithms. We tested the proven results by applying a two dimensional simple random walk to factoring integers and proved them trustable.

This paper introduces our research work. In section 2, we give the definition of the Cartesian subtraction; in section 3, we prove 7 lemmas, 3 theorems, and 7 corollaries; in section 4, we explore the application of the proven results to integer factorization; in section 5, we presents our future work and hopes.

2 Preliminaries

This section presents necessary symbols, notations, definitions, and fundamental knowledge for later investigation.

2.1 Classical Terminologies and Symbols

In this whole paper, a set is assumed to be finite, countable, unordered, and to have subtraction operation related with its elements. Symbols $\emptyset$,$\cup$,$-$, and $\in$, which are used to operate on sets, are used as their usual meanings introduced in the textbooks. Particularly, $A - B$ means removing from A all the elements that are also in B. Symbol $A \Rightarrow B$ means conclusion B can be derived from condition A, or we can reason from A to B. Symbols $\lfloor x \rfloor$ and $\lceil x \rceil$ are respectively the floor and ceil functions such that $x - 1 < \lfloor x \rfloor \leqslant x \leqslant \lceil x \rceil < x + 1$ or $x = \lfloor x \rfloor + \{x\} = \lceil x \rceil - 1 + \{x\}$, where $\{x\}$ is the fractional part of x. Symbol $x = a \bmod b$ means x is the remainder of a dividing by b, namely, $a = kb + x$, where a, b, k, and x are all integers.

2.2 New Notations

Let S be a finite set and $e \in S$; the number of e is called the multiplicity of e and denoted with m_e. For example, $S = \{1, 2, 2, 3\} \Rightarrow m_1 = 1, m_2 = 2$, and $m_3 = 1$. Symbol $e^{\vee m}$ means e repeated by m times and placed together without considering their orders, namely, $e^{\vee m} = \underbrace{e, e, ..., e}_{m \quad times}$. By this means, $S = \{1, 2, 3, 2\} = \{1^{\vee 1}, 2^{\vee 2}, 3^{\vee 1}\}$. Let $X = \{x_1, x_2, ..., x_n\}$ be a finite set containing $n > 0$ elements; symbol X^k with integer $k > 0$ means the set

$$\{\underbrace{x_1, x_1, ..., x_1}_{k \quad times}, \underbrace{x_2, x_2, ..., x_2}_{k \quad times}, ..., \underbrace{x_n, x_n, ..., x_n}_{k \quad times}\} = \{x_1^{\vee k}, x_2^{\vee k}, ..., x_n^{\vee k}\} = \{x_1^{\vee k}\} \cup \{x_2^{\vee k}\} \cup ... \cup \{x_n^{\vee k}\}$$

Let $A = \{a_1, a_2, ..., a_n\}$ be a finite set of n integers, where $n \geq 0$ is an integer; then $-A = \{-a_1, -a_2, ..., -a_n\}$, and $B = A(\mathrm{mod} X)$ means $B = \{a_1 \bmod X, a_2 \bmod X, ..., a_n \bmod X\}$, where X is an integer . If $B = \{b_1, b_2, ..., b_n\}$ is a set of n integers, $B \equiv A(\mathrm{mod} X)$ means $b_i \equiv a_i(\mathrm{mod} X)$ for $i = 1, 2, ..., n$.

An integer interval $[a, b]$ means the set of all the integers bounded with a and b with $a < b$; for example, integer interval $[5, 9] = \{5, 6, 7, 8, 9\}$. An old integer interval $[a, b]$ means the set of all the odd integers bounded with odd integers a and b with $a < b$; for example, odd integer interval $[5, 9] = \{5, 7, 9\}$. If an integer interval contains integer x, that integer interval is called a host interval of x. If d is a divisor of integer n, n is called a host number of d or a number hosting d.

2.3 New Definitions

Definition 2.1. Let $X = \{x_1, x_2, ..., x_n\}$ be a finite set, where $n \geq 0$ is an integer; X is called a zero set if each of its elements is zero, namely, $X = \underbrace{\{0, 0, ..., 0\}}_{n \quad ones}$. Use $X = 0$ to indicate X is a zero set.

Definition 2.2. Let $A = \{a_1, a_2, ..., a_s\}$ and $B = \{b_1, b_2, ..., b_t\}$, where s and t are positive integers; the Cartesian subtraction $B \ominus A$ is defined to be the set

$$B \ominus A = \{b_i - a_j | b_i \in B, a_j \in A, 1 \leq i \leq t, 1 \leq j \leq s\}$$

For convenience, it is simply denoted by

$$B \ominus A = \{b_i - a_j | b_i \in B, a_j \in A\}$$

Obviously, $B \ominus A \neq \emptyset$.

Remark 2.1. 'Cartesian subtraction' is named by referring to the terminology 'Cartesian product' , which can be found in many literatures, e.g., Eric's book [10]. Seen at page 2670 of [10], the Cartesian product of two sets A and B is defined to be the set of all points (a, b) where $a \in A$ and $b \in B$. According to this concept, we have Definition 2.2. Likewise, we can also define the Cartesian sum of two sets by

$$A \oplus B = \{a_j + b_i | a_j \in A, b_i \in B\}$$

However, this paper merely concerns the Cartesian subtraction.

Definition 2.3. Let $A = \{a_1, a_2, ..., a_n\}$ be a finite set, where n is a positive integer. The set $\tilde{A}$ formed by all the distinct terms in A is called the core of A. For example, $A = \{1, 2, 2, 3\} \Rightarrow \tilde{A} = \{1, 2, 3\}$.

3 Main Results

We have obtained several lemmas to describe the properties of $B \ominus A$ in the general case; we also obtain several theorems and corollaries related to the sets of integers.

3.1 General Properties

Lemma 3.1. *Assume $A = \{a\}, B = \{b\}$, and $C = \{c_1, c_2, ..., c_n\}$, where $n > 0$ is an integer; let $C_A = C \ominus A$ and $C_B = C \ominus B$; then*

$$C_A \cup C_B = \{c_i - x_j|, c_i \in C, x_j \in A \cup B\}$$

or

$$(C \ominus A) \cup (C \ominus B) = C \ominus (A \cup B)$$

Proof. Direct calculations show

$$\begin{array}{l} \left\{ \begin{array}{l} C_A = \{c_1 - a, c_2 - a, ..., c_n - a\} \\ C_B = \{c_1 - b, c_2 - b, ..., c_n - b\} \end{array} \right. \Rightarrow C_A \cup C_B \\ = \{c_1 - a, c_2 - a, ..., c_n - a, c_1 - b, c_2 - b, ..., c_n - b\} \end{array}$$

Let $X = \{c_i - x_j|, c_i \in C, x_j \in A \cup B\}$; then

$$X = \{c_1 - a, c_2 - a, ..., c_n - a, c_1 - b, c_2 - b, ..., c_n - b\}$$

As a result,

$$C_A \cup C_B = X$$

establishing the lemma. □

Lemma 3.2. *Assume* $A_1 = \{a_1\}$,$A_2 = \{a_2\}$, $A = \{a_1, a_2\} = A_1 \cup A_2$, *and* $B = \{b_1, b_2, ..., b_n\}$, *where* $n > 0$ *is an integer; let*

$$C_1 = B \ominus A_1 = \{b_i - a_1|, b_i \in B, a_1 \in A\}, C_2 = B \ominus A_2 = \{b_i - a_2|, b_i \in B, a_2 \in A\}$$

and

$$C = B \ominus A = \{b_i - a_j|, b_i \in B, a_j \in A\}$$

then

$$C = C_1 \cup C_2$$

or

$$B \ominus A = (B \ominus A_1) \cup (B \ominus A_2)$$

Proof. This lemma is an alternative statement of Lemma 3.1. Thus the proof is the same as that to prove Lemma 3.1. □

Lemma 3.3. *Assume* $A = A_1 \cup A_2$ *and* $B = B_1 \cup B_2$, *where*A_1, A_2, B_1, *and* B_2 *are nonempty sets; then*

$$B \ominus A = \underset{i,j=1,2}{\cup}(B_i \ominus A_j)$$

More generally, $A = A_1 \cup A_2 \cup ... \cup A_k$ *and* $B = B_1 \cup B_2 \cup ... \cup B_l$ *yields*

$$B \ominus A = \cup(B_i \ominus A_j)$$

where k *and* l *are positive integers,* $A_i \neq \emptyset$, *and* $B_j \neq \emptyset$ *for* $1 \leq i \leq l$ *and* $1 \leq j \leq k$.

Proof. . Without loss of generality, assume $A_1 = \{a_{11}, a_{12}, ..., a_{1s}\}, A_2 = \{a_{21}, a_{22}, ..., a_{2t}\}$, $B_1 = \{b_{11}, b_{12}, ..., b_{1u}\}$, and $B_2 = \{b_{21}, b_{22}, ..., b_{2v}\}$, where s, t, u, and v are positive integers; let $C = B \ominus A$; then by definition

$$B \ominus A = \{b_{1i} - a_{1x}, b_{1i} - a_{2y}, b_{2j} - a_{1x}, b_{2j} - a_{2y}|b_{1i}, b_{2j} \in B, a_{1x}, a_{2y} \in A, \\ 1 \leq i \leq u, 1 \leq j \leq v, 1 \leq x \leq s, 1 \leq y \leq t\}$$

Since

$$B_1 \ominus A_1 = \{b_{1i} - a_{1x}|b_{1i} \in B, a_{1x} \in A, 1 \leq i \leq u, 1 \leq x \leq s\}$$

$$B_1 \ominus A_2 = \{b_{1i} - a_{2y}|b_{1i} \in B, a_{2y} \in A, 1 \leq i \leq u, 1 \leq y \leq t\}$$

$$B_2 \ominus A_1 = \{b_{2j} - a_{1x}|b_{2j} \in B, a_{1x} \in A, 1 \leq j \leq v, 1 \leq x \leq s\}$$

and

$$B_2 \ominus A_2 = \{b_{2j} - a_{2y}|, b_{2j} \in B, a_{2y} \in A, 1 \leq j \leq v, 1 \leq y \leq t\}$$

it is sure $B \ominus A = \underset{i,j=1,2}{\cup}(B_i \ominus A_j)$.

The general case is proven in the same way. □

Lemma 3.4. *Assume* $A = \{a\}$, $B = \{a, a\}$ *and* $C = \{c_1, c_2, ..., c_n\}$, *where* $n > 0$ *is an integer. Let*

$$C_A = C \ominus A = \{c_i - a|, c_i \in C, a \in A\}$$

and

$$C_B = C \ominus B = \{c_i - x_j|, c_i \in C, x_j \in B\}$$

then

$$C_B = C_A^2$$

or

$$C \ominus B = C \ominus A^2 = (C \ominus A)^2$$

More generally, $A = \{a\}$ *and* $X = \{\underbrace{a, a, ..., a}_{k \quad ones}\}$ *yield* $C \ominus X = C_A^k$ *or*

$$C \ominus X = C \ominus A^k = (C \ominus A)^k$$

Proof. Direct calculations show

$$\begin{cases} C_A = \{c_1 - a, c_2 - a, ..., c_n - a\} \\ C_B = \{c_1 - a, c_1 - a, c_2 - a, c_2 - a..., c_n - a, c_n - a\} \end{cases} \Rightarrow C_B = C_A^2$$

Since $B = A^2$, it follows

$$C \ominus B = C \ominus A^2 = (C \ominus A)^2$$

Since $X = A^k$, it holds

$$C \ominus X = C \ominus A^k = \{(c_1 - a)^{\vee k}, (c_2 - a)^{\vee k}, ..., (c_n - a)^{\vee k}\} = C_A^k = (C \ominus A)^k$$

□

Lemma 3.4*. Assume $A = \{a\}$,$B = \{a, a\}$ and $C = \{c_1, c_2, ..., c_n\}$, where $n > 0$ is an integer. Let

$$C_A = A \ominus C = \{a - c_i|, c_i \in C, a \in A\}$$

and

$$C_B = B \ominus C = \{x_j - c_i|, c_i \in C, x_j \in B\}$$

then

$$C_B = C_A^2$$

or

$$B \ominus C = A^2 \ominus C = (A \ominus C)^2$$

More generally, $A = \{a\}$ and $X = \{\underbrace{a, a, ..., a}_{k \quad ones}\}$ yield $X \ominus C = C_A^k$ or

$$X \ominus C = A^k \ominus C = (A \ominus C)^k$$

Proof. Direct calculations show

$$\begin{cases} C_A = \{a - c_1, a - c_2, ..., a - c_n\} \\ C_B = \{a - c_1, a - c_1, a - c_2, a - c_2..., a - c_n, a - c_n\} \end{cases} \Rightarrow C_B = C_A^2$$

Hence it follows

$$C \ominus B = C \ominus A^2 = (C \ominus A)^2$$

Since $X = A^k$, it holds

$$X \ominus C = A^k \ominus C = \{(a - c_1)^{\vee k}, (a - c_2)^{\vee k}, ..., (a - c_n)^{\vee k}\} = C_A^k = (A \ominus C)^k$$

□

Lemma 3.5. *Assume $A = \{a\}$ and $B = \{b_1, b_2, ..., b_n\}$, where $n > 0$ is an integer; then*

$$(A \ominus B)^k = -(B \ominus A)^k$$

where $k > 0$ is an integer.

Proof. Comparison to the proofs of Lemma 3.4 and Lemma 3.4* immediately results in this lemma. □

Lemma 3.6. *Assume $A = \{a\}, B = \{b\}$ and $C = \{c\}$; then*

$$(C \ominus A^g) \cup (C \ominus B^g) = ((C \ominus A) \cup C \ominus B))^g$$

where g is a positive integer.

Proof. Since $A^g = \{\underbrace{a, a, ..., a}_{g \quad times}\}$ and $B^g = \{\underbrace{b, b, ..., b}_{g \quad times}\}$, direct calculations show

$$\begin{cases} C \ominus A^g = \{\underbrace{c-a, c-a, ..., c-a}_{g \quad times}\} = \{(c-a)^{\vee g}\} \\ C \ominus B^g = \{\underbrace{c-b, c-b, ..., c-b}_{g \quad times}\} == \{(c-b)^{\vee g}\} \end{cases}$$
$$\Rightarrow (C \ominus A^g) \cup (C \ominus A^g) = \{(c-a)^{\vee g}, (c-b)^{\vee g}\} = ((C \ominus A) \cup (C \ominus B))^g$$

□

Lemma 3.7. *Assume $A = \{\underbrace{a, a, ..., a}_{p \quad ones}\}$ and $B = \{\underbrace{b, b, ..., b}_{q \quad ones}\}$, where p and q are positive integers. Let*

$$C = B \ominus A = \{b_i - a_j|, b_i \in B, a_j \in A\}$$

then

$$C = \{(b-a)^{\vee pq}\}$$

Proof. . Direct calculations show

$$C = \{\underbrace{(b-a)^{\vee p}, (b-a)^{\vee p}, ..., (b-a)^{\vee p}}_{q \quad ones}\} = \{(b-a)^{\vee pq}\}$$

□

3.2 Properties Related to Integer Sets

Theorem 3.8. *Let k and l be two positive integers, $\alpha = \min(k, l)$, and $\beta = \max(k, l)$; assume $A = \{a_1, a_2, ..., a_k\}$ and $B = \{b_1, b_2, ..., b_l\}$ are two sets of consecutive integers such that $b_1 - a_k = \omega \geq 0$; let C be the Cartesian subtraction $B \ominus A$ defined by*

$$C = B \ominus A = \{c_{ij} = b_i - a_j | b_i \in B, a_j \in A\}$$

then the following statements hold:

1. *The element c_{ij} is calculated by*

$$c_{ij} = b_i - a_j = \omega + (i-1) + (k-j), i = 1, 2, ..., l; j = 1, 2, ..., k. \tag{3.1}$$

Consequently, C contains kl elements among which the smallest one is ω, the biggest one is $\omega + (l\text{-}1)+(k\text{-}1)$.

2. *There are in C totally $k + l - 1$ distinct elements, which are ω, $\omega+1$,. . . , and $\omega + (l\text{-}1)+(k\text{-}1)$. Accordingly, there are certain duplicative elements in C and the multiplicity of each element is given by*

$$\begin{array}{l} m_\omega = 1, m_{\omega+1} = 2, ..., m_{\omega+\alpha-2} = \alpha - 1, \\ m_{\omega+\alpha-1} = ... = m_{\omega+\beta-1} = \alpha, \\ m_{\omega+\beta} = \alpha - 1, m_{\omega+\beta+1} = \alpha - 2, ..., m_{\omega+\beta+\alpha-3} = 2, m_{\omega+\beta+\alpha-2} = 1. \end{array} \tag{3.2}$$

That is to say, among the $k + l$-1 distinct elements in C, there are $\beta - \alpha + 1$ ones with multiplicity α, 2 ones with multiplicity α-1, 2 ones with multiplicity α-2, and so forth, 2 ones with multiplicity 1.

Proof. Since A and B are sets of consecutive positive integers, it knows $b_i = b_1 + i - 1$ and $a_j = a_1 + j - 1 = a_k - k + j$. Consequently, it holds

$$b_i - a_j = b_1 + i - 1 - (a_k - k + j) = b_1 - a_k + (i-1) + k - j = \omega + (i-1) + (k-j)$$

which is just the formula (3.1).

Now writing C in the following form of rows and columns

$$C = \left\{ \begin{array}{lllll} b_1 - a_1, & b_1 - a_2, & b_1 - a_3, & ... & b_1 - a_k, \\ b_2 - a_1, & b_2 - a_2, & b_2 - a_3, & ... & b_2 - a_k, \\ ... & ... & ... & ... & ... \\ b_l - a_1, & b_l - a_2, & b_l - a_3, & ... & b_l - a_k \end{array} \right\}$$

If $k = l$, it yields

$$C = \left\{ \begin{array}{lllll} \omega + k - 1, & \omega + k - 2, & \omega + k - 3, & ... & \omega, \\ \omega + k & \omega + k - 1, & \omega + k - 2, & ... & \omega + 1, \\ ... & ... & ... & ... & ... \\ \omega + 2k - 2, & \omega + 2k - 3, & \omega + 2k - 4, & ... & \underline{c_{kk} = \omega + k - 1} \end{array} \right\} \tag{3.3}$$

If $k < l$, it follows

$$C = \left\{ \begin{array}{llll} \omega + k - 1, & \omega + k - 2, & \omega + k - 3, & ... \quad \omega, \\ \omega + k & \omega + k - 1, & \omega + k - 2, & ... \quad \omega + 1, \\ ... & ... & ... & ... \quad ... \\ \omega + 2k - 2, & \omega + 2k - 3, & \omega + 2k - 4, & ... \quad \underline{c_{kk} = \omega + k - 1}, \\ \omega + 2k - 1, & \omega + 2k - 2, & \omega + 2k - 3, & ... \quad \omega + k, \\ ... & ... & ... & ... \quad ... \\ \omega + l - 1 + k - 1, & \omega + l - 1 + k - 2, & \omega + l - 1 + k - 3, & ... \quad \underline{c_{lk} = \omega + l - 1} \end{array} \right\} \tag{3.4}$$

If $k > l$, it follows

$$C = \left\{ \begin{array}{llllll} \omega + k - 1 & \omega + k - 2 & ... & \omega + k - l & \omega + k - l - 1 & ... \quad \omega \\ \omega + k & \omega + k - 1 & ... & \omega + k - l + 1 & \omega + k - l & ... \quad \omega + 1 \\ ... & ... & ... & ... & ... & ... \quad ... \\ \omega + k + l - 2 & \omega + k + l - 3 & .. & \underline{c_{ll} = \omega + k - 1} & \omega + k - 2 & ... \quad \underline{c_{lk} = \omega + l - 1} \end{array} \right\} \tag{3.5}$$

The formulas (3.3), (3.4) ,and (3.5) obviously show that C contains *kl* elements among which ω is the smallest one and $\omega + (l\text{-}1)+(k\text{-}1)$ is the biggest one. The formulas (3.3), (3.4) ,and (3.5) also prove the law revealed in (3.2). □

Remark 3.1. In (3.3),(3.4), and (3.5), C is orderly expressed in terms of its elements. Without considering the order of the elements, for the case $k \neq l$, C is expressed by

$$C = \{\omega^{\vee 1}, (\omega+1)^{\vee 2}, ..., (\omega+\alpha-2)^{\vee(\alpha-1)}, (\omega+\alpha-1)^{\vee\alpha}, (\omega+\alpha)^{\vee\alpha}, ..., (\omega+\beta-1)^{\vee\alpha}, (\omega+\beta)^{\vee(\alpha-1)}, \\ ..., (\omega+\beta+\alpha-3)^{\vee 2}, (\omega+\beta+\alpha-2)^{\vee 1}\}$$

For the case $k = l$, it yields

$$C = \{\omega^{\vee 1}, (\omega+1)^{\vee 2}, ..., (\omega+\alpha-2)^{\vee(\alpha-1)}, (\omega+\alpha-1)^{\vee\alpha}, (\omega+\alpha)^{\vee(\alpha-1)}, ..., (\omega+2\alpha-3)^{\vee 2}, (\omega+2\alpha-2)^{\vee 1}\}$$

Let m_x, where $x \in C$, be the *multiplicity function* on C; then its graph is depicted as Figure 1.

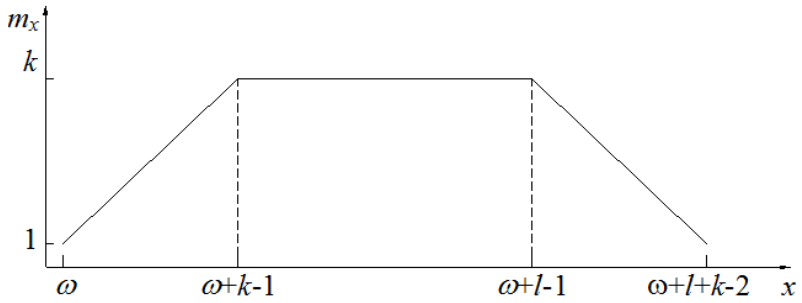

Figure 1: Graph of m_x with $l \geq k > 0$

Example 3.9. *Let* $A = \{1, 2, 3, 4\}$ *and* $B = \{5, 6, 7, 8\}$*; then* $k = 4$, $l = 4$, $\omega = 1$, *and*

$$C = \{4, 3, 2, 1, 5, 4, 3, 2, 6, 5, 4, 3, 7, 6, 5, 4\} = \{1^{\vee 1}, 2^{\vee 2}, 3^{\vee 3}, 4^{\vee 4}, 5^{\vee 3}, 6^{\vee 2}, 7^{\vee 1}\}$$

It can be seen that, the number 4 appears 4 times, the number 3 appears 3 times and the number 2 appears 2 times. That is $m_1 = 1$, $m_2 = 2$, $m_3 = 3$, $m_4 = 4$, $m_5 = 3$, $m_6 = 2$, *and* $m_1 = 7$.

Example 3.10. *Let* $A = \{1, 2, 3, 4\}$ *and* $B = \{4, 5, 6, 7\}$*; then* $k = 4$, $l = 4$, $\omega = 0$, *and*

$$C = \{3, 2, 1, 0, 4, 3, 2, 1, 5, 4, 3, 2, 6, 5, 4, 3\} = \{0^{\vee 1}, 1^{\vee 2}, 2^{\vee 3}, 3^{\vee 4}, 4^{\vee 3}, 5^{\vee 2}, 6^{\vee 1}\}$$

Hence $m_0 = 1, m_1 = 2, m_2 = 3, m_3 = 4, m_4 = 3, m_5 = 2$, *and* $m_6 = 1$.

Example 3.11. *Let* $A = \{1, 2, 3\}$ *and* $B = \{5, 6, 7, 8\}$*; then* $k = 3$, $l = 4$, $\omega = 2$, *and*

$$C = \{4, 5, 6, 7, 3, 4, 5, 6, 2, 3, 4, 5\} = \{2^{\vee 1}, 3^{\vee 2}, 4^{\vee 3}, 5^{\vee 3}, 6^{\vee 2}, 7^{\vee 1}\}$$

Hence $m_2 = 1, m_3 = 2, m_4 = 3, m_5 = 3, m_6 = 2$, *and* $m_7 = 1$.

Example 3.12. *Let* $A = \{-3, -2, -1\}$ *and* $B = \{0, 1, 2, 3\}$*; then* $k = 3$, $l = 4$, $\omega = 1$, *and*

$$C = \{3, 4, 5, 6, 2, 3, 4, 5, 1, 2, 3, 4\} = \{1^{\vee 1}, 2^{\vee 2}, 3^{\vee 3}, 4^{\vee 3}, 5^{\vee 2}, 6^{\vee 1}\}$$

Hence $m_1 = 1, m_2 = 2, m_3 = 3, m_4 = 3, m_5 = 2$, *and* $m_6 = 1$.

Example 3.13. *Let* $A = \{-4, -3, -2, -1\}$ *and* $B = \{1, 2, 3, 4\}$*; then* $k = 3$, $l = 4$, $\omega = 2$, *and*

$$C = \{5, 4, 3, 2, 6, 5, 4, 3, 7, 6, 5, 4, 8, 7, 6, 5\} = \{2^{\vee 1}, 3^{\vee 2}, 4^{\vee 3}, 5^{\vee 4}, 6^{\vee 3}, 7^{\vee 2}, 8^{\vee 1}\}$$

Hence $m_2 = 1, m_3 = 2, m_4 = 3, m_5 = 4, m_6 = 3, m_7 = 2$, *and* $m_8 = 1$.

Example 3.14. *Let* $A = \{-3, -2, -1\}$ *and* $B = \{0, 1, 2, 3, 4\}$*; then* $k = 4$*,* $l = 5$*,* $\omega = 1$*, and*

$$C = \{3, 4, 5, 6, 7, 2, 3, 4, 5, 6, 1, 2, 3, 4, 5\} = \{1^{\vee 1}, 2^{\vee 2}, 3^{\vee 3}, 4^{\vee 3}, 5^{\vee 3}, 6^{\vee 2}, 7^{\vee 1}\}$$

Hence $m_1 = 1, m_2 = 2, m_3 = 3, m_4 = 3, m_5 = 3, m_6 = 2$*, and* $m_7 = 1$*.*

Example 3.15. *Let* $A = \{1, 2, 3, 4, 5, 6\}$ *and* $B = \{7, 8, 9, 10\}$*; then* $k = 6$*,* $l = 4$*,* $\omega = 1$*,*

$$\begin{aligned} C &= \{6, 5, 4, 3, 2, 1, 7, 6, 5, 4, 3, 2, 8, 7, 6, 5, 4, 3, 9, 8, 7, 6, 5, 4\} \\ &= \{1^{\vee 1}, 2^{\vee 2}, 3^{\vee 3}, 4^{\vee 4}, 5^{\vee 4}, 6^{\vee 4}, 7^{\vee 3}, 8^{\vee 2}, 9^{\vee 1}\} \end{aligned}$$

Hence $m_1 = 1, m_2 = 2, m_3 = 3, m_4 = 4, m_5 = 4, m_6 = 4, m_7 = 3, m_8 = 2$*, and* $m_9 = 1$*.*

Corollary 3.16. *Let* k*,* l*,* A*,* B *and* C *be defined as those in Theorem 3.8; if* $A = B$*, then*

1. *The elements in* C *are list in rows and columns by*

$$C = \begin{Bmatrix} 0, & -1, & -2, & ..., & 1-k, \\ 1, & 0, & -1, & ... & 2-k, \\ ... & ... & ... & ... & ... \\ k-1, & k-2, & k-3, & ... & 0 \end{Bmatrix} \tag{3.6}$$

   or

$$C = \{(1-k)^{\vee 1}, (2-k)^{\vee 2}, ..., -1^{\vee(k-1)}, 0^{\vee k}, 1^{\vee(k-1)}, 2^{\vee(k-2)}, ..., (k-2)^{\vee 2}, (k-1)^{\vee 1}\} \tag{3.7}$$

   which leads to $m_{1-k} = 1, m_{2-k} = 2, ..., m_{-p} = k - p, ...,$*,* $m_{-2} = k - 2$*,* $m_{-1} = k - 1$*,* $m_0 = k$*,* $m_1 = k - 1$*,*$m_2 = k - 2$*,...,* $m_p = k - p$*,...,*$m_{k-2} = 2$*, and* $m_{k-1} = 1$*.*

2. *There are* k *elements between two repeated elements that take the same value.*

Proof. The condition $A = B$ yields $\omega = 1 - k$. This and (3.3) soon result in (3.6) and (3.7). The list (3.6) also establishes the conclusion 2. □

Remark 3.2. Consider $\hat{C}$ such that $\hat{c}_{ij} = |c_{ij}|$, where $\hat{c}_{ij} \in \hat{C}$; then

$$\hat{C} = \{0^{\vee k}, 1^{\vee 2(k-1)}, 2^{\vee 2(k-2)}, ..., p^{\vee 2(k-p)}, ..., (k-2)^{\vee 4}, (k-1)^{\vee 2}\} \tag{3.8}$$

Corollary 3.17. *Let* α*,* β*,* ω*,* A*, and* B *be defined as those in Theorem 3.8, and* $\hat{C}$ *be defined with* $\hat{c}_{ij} = |c_{ij}|$*; then when* $B = A$ *there are totally* k^2 *elements in* $\hat{C}$ *among which there are* $2(k - s)$ *ones take value* s*, where* s *is an integer with* $0 < s \leq k - 1$*.*

Proof. Let $C = B \ominus A$. By Theorem 3.8, C contains k^2 elements when $B = A$. Hence $\hat{C}$ contains k^2 elements because it has the same number of elements as C has. The second conclusion is seen in (3.8). □

Example 3.18. *Let* $A = \{1, 2, 3, 4\}$ *and* $B = \{1, 2, 3, 4\}$*; then*

$$\begin{aligned} C &= \{0, -1, -2, -3, 1, 0, -1, -2, 2, 1, 0, -1, 3, 2, 1, 0\} \\ &= \{-3^{\vee 1}, -2^{\vee 2}, -1^{\vee 3}, 0^{\vee 4}, 1^{\vee 3}, 2^{\vee 2}, 3^{\vee 1}\} \\ \Rightarrow \hat{C} &= \{0^{\vee 4}, 1^{\vee 6}, 2^{\vee 4}, 3^{\vee 2}\} \end{aligned}$$

Corollary 3.19. *Let* $A = [a + 1, a + j]$*,* $B = [a + j + 1, a + j + k]$*,* $C = [a + j + k + 1, a + j + k + l]$ *be integer intervals, and* $S = A \cup B \cup C$*, where* a *is an integer,* $j \geq 1$*,* $k \geq 1$*, and* $l \geq 1$ *; then*

$$\begin{aligned} S \ominus S = \{&(1 - j - k - l)^{\vee 1}, ..., -j^{\vee(k+l)} ..., -1^{\vee(j+k+l-1)}, 0^{\vee(j+k+l)}, 1^{\vee(j+k+l-1)}, ..., \\ &j^{\vee(k+l)}, (j+1)^{\vee(k+l-1)}, (j+2)^{\vee(k+l-2)}, ..., (j+k)^{\vee l}, ..., (j+k+l-1)^{\vee 1}\} \end{aligned}$$

Let $\hat{S} = \{|e_{ij}||e_{ij} \in S \ominus S\}$*; then*

$$\hat{S} = \{0^{\vee(j+k+l)}, 1^{\vee 2(j+k+l-1)}, ..., j^{\vee 2(k+l)}, (j+1)^{\vee 2(k+l-1)}, (j+2)^{\vee 2(k+l-2)}, ..., (j+k)^{\vee 2l}, ..., (j+k+l-1)^{\vee 2}\}$$

Proof. The conclusions are directly from (3.7) and (3.8). □

Remark 3.3. Taking $a = 0$ in Corollary 3.19 results in $A = [1, j]$, $B = [j + 1, j + k]$, $C = [j + k + 1, j + k + l]$, and $S = [1, j + k + l]$. It is seen that, the bigger k and l are, the more multiplicity of the elements from $[1, j - 1]$ and $[j, j + k]$.

Example 3.20. *Let* $A = \{1, 2, 3, 4\}$, $B = \{5, 6, 7\}$, $C = \{8, 9, 10, 11\}$*; then* $a = 0$, $j = 4$, $k = 3$, $l = 4$, *and* $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$,

$$S \ominus S = \left\{ \begin{array}{ccccccccccc} 0, & -1, & -2, & -3, & -4, & -5, & -6, & -7, & -8, & -9, & -10, \\ 1, & 0, & -1, & -2, & -3, & -4, & -5, & -6, & -7, & -8, & -9, \\ 2, & 1, & 0, & -1, & -2, & -3, & -4, & -5, & -6, & -7, & -8, \\ 3, & 2, & 1, & 0, & -1, & -2, & -3, & -4, & -5, & -6, & -7, \\ 4, & 3, & 2, & 1, & 0, & -1, & -2, & -3, & -4, & -5, & -6, \\ 5, & 4, & 3, & 2, & 1, & 0, & -1, & -2, & -3, & -4, & -5, \\ 6, & 5, & 4, & 3, & 2, & 1, & 0, & -1, & -2, & -3, & -4, \\ 7, & 6, & 5, & 4, & 3, & 2, & 1, & 0, & -1, & -2, & -3, \\ 8, & 7, & 6, & 5, & 4, & 3, & 2, & 1, & 0, & -1, & -2, \\ 9, & 8, & 7, & 6, & 5, & 4, & 3, & 2, & 1, & 0, & -1, \\ 10, & 9, & 8, & 7, & 6, & 5, & 4, & 3, & 2, & 1, & 0 \end{array} \right\}$$
$$= \{-10^{\vee 1}, -9^{\vee 2}, -8^{\vee 3}, -7^{\vee 4}, -6^{\vee 5}, -5^{\vee 6}, -4^{\vee 7}, -3^{\vee 8}, -2^{\vee 9}, -1^{\vee 10}, 0^{\vee 11}, 1^{\vee 10}, 2^{\vee 9}, 3^{\vee 8}, 4^{\vee 7}, 5^{\vee 6}, 6^{\vee 5}, 7^{\vee 4}, 8^{\vee 3}, 9^{\vee 2}, 10^{\vee 1}\}$$

and

$$\hat{S} = \{0^{\vee 11}, 1^{\vee 20}, 2^{\vee 18}, 3^{\vee 16}, 4^{\vee 14}, 5^{\vee 12}, 6^{\vee 10}, 7^{\vee 8}, 8^{\vee 6}, 9^{\vee 4}, 10^{\vee 2}\}$$

Corollary 3.21. *Let* a *be an integer; taking* $A = \{a\}$, $B = \{a + 1, ..., a + k\}$, $C = \{a + k + 1, a + k + 2, ..., a + k + l\}$, *and* $S = A \cup B \cup C$, *where* $k \geq 1$ *and* $l \geq 1$ *are integers; then*

$$S \ominus S = \{-(k+l)^{\vee 1}, -k^{\vee (l+1)}, ..., -2^{\vee (k+l-1)}, -1^{\vee (k+l)}, 0^{\vee (k+l+1)}, 1^{\vee (k+l)}, 2^{\vee (k+l-1)}, ..., k^{\vee (l+1)}, ..., (k+l)^{\vee 1}\}$$

Let $\hat{S} = \{|e_{ij}||e_{ij} \in S \ominus S\}$*; then*

$$\hat{S} = \{0^{\vee (k+l+1)}, 1^{\vee 2(k+l)}, 2^{\vee 2(k+l-1)}, ..., k^{\vee 2(l+1)}, ..., (k + l)^{\vee 2}\}$$

Proof. (Omitted). □

Theorem 3.22. *Let* A *and* B *be defined as those in Theorem 3.8; then for positive integer* g*, it holds*

$$B \ominus A^g = (B \ominus A)^g$$

and

$$A^g \ominus B = (A \ominus B)^g$$

Proof. Let $A_i = \{a_i\}$ with $i = 1, 2, ..., k$ and $B_j = \{b_j\}$ with $j = 1, 2, ..., l$; then $A = \underset{1 \leq i \leq k}{\cup} A_i$, $B = \underset{1 \leq j \leq l}{\cup} B_i$, $A_i^g = \{\underbrace{a_i, a_i, ..., a_i}_{g \quad times}\}$, and $A^g = \underset{1 \leq i \leq k}{\cup} A_i^g$.

Since

$$B \ominus A^g = B \ominus (\underset{1 \leq i \leq k}{\cup} A_i^g) = (\underset{1 \leq j \leq k}{\cup} B_j) \ominus (\underset{1 \leq i \leq k}{\cup} A_i^g)$$

By Lemmas 3.2, 3.3, 3.4 and 3.6, it holds

$$B \ominus A^g = \underset{1 \leq j \leq k}{\cup} (B_j \ominus (\underset{1 \leq i \leq k}{\cup} A_i^g)) = \underset{1 \leq j \leq k}{\cup} (B_j \ominus (\underset{1 \leq i \leq k}{\cup} A_i))^g = \underset{1 \leq j \leq k}{\cup} (B_j \ominus A)^g = (B \ominus A)^g$$

Similarly, it holds

$$A^g \ominus B = (A \ominus B)^g$$

□

Example 3.23. *Let* $A = \{1, 2, 3, 4\}$,$\hat{A} = A^2 = \{1, 1, 2, 2, 3, 3, 4, 4\}$ *and* $\hat{B} = \{5, 6, 7, 8\}$*; then* $k = 4, l = 4$ *and* $g = 2$*; direct calculations show*

$$\begin{aligned}\hat{B} \ominus A^2 &= \{4, 4, 3, 3, 2, 2, 1, 1, 5, 5, 4, 4, 3, 3, 2, 2, 6, 6, 5, 5, 4, 4, 3, 3, 7, 7, 6, 6, 5, 5, 4, 4\} \\ &= \{1^{\vee 2}, 2^{\vee 4}, 3^{\vee 6}, 4^{\vee 8}, 5^{\vee 6}, 6^{\vee 4}, 7^{\vee 2}\}\end{aligned}$$

and

$$\begin{aligned}A^2 \ominus \hat{B} = \{&-4, -5, -6, -7, -4, -5, -6, -7, -3, -4, -5, -6, -3, -4, -5, -6, \\ &-2, -3, -4, -5, -2, -3, -4, -5, -1, -2, -3, -4, -1, -2, -3, -4\} \\ = \{&-1^{\vee 2}, -2^{\vee 4}, -3^{\vee 6}, -4^{\vee 8}, -5^{\vee 6}, -6^{\vee 4}, -7^{\vee 2}\}\end{aligned}$$

Compared to Example 3.9, this example demonstrates what Theorem 3.22 claims.

Corollary 3.24. *Let* $A = \{a_1, a_2, ..., a_k\}$ *be a set of consecutive integers; then*

$$A^g \ominus A^g = (A \ominus A)^{g^2} = \{(a_i - a_j)^{\vee g^2} | a_i, a_j \in A, 1 \le i, j \le k\}$$

where k *and* g *are positive integers.*

Proof. Let $\hat{A} = \hat{B} = A^g$ and

$$\hat{C} = \hat{B} \ominus \hat{A} = \{c_{ij} | c_{ij} = b_i - a_j, b_i \in \hat{B}, a_j \in \hat{A}\}$$

then $\hat{A}$ and $\hat{B}$ are given by

$$\hat{A} = \{\underbrace{a_1, a_1, ..., a_1}_{g \quad times}, \underbrace{a_2, a_2, ..., a_2}_{g \quad times}, ..., \underbrace{a_k, a_k, ..., a_k}_{g \quad times}\}$$

and

$$\hat{B} = \{\underbrace{a_1, a_1, ..., a_1}_{g \quad times}, \underbrace{a_2, a_2, ..., a_2}_{g \quad times}, ..., \underbrace{a_k, a_k, ..., a_k}_{g \quad times}\}$$

Let

$$A_1 = \{\underbrace{a_1, a_1, ..., a_1}_{g \quad times}\}, A_2 = \{\underbrace{a_2, a_2, ..., a_2}_{g \quad times}\}, ..., A_k = \{\underbrace{a_k, a_k, ..., a_k}_{g \quad times}\}$$

and

$$B_1 = \{\underbrace{a_1, a_1, ..., a_1}_{g \quad times}\}, B_2 = \{\underbrace{a_2, a_2, ..., a_2}_{g \quad times}\}, ..., B_k = \{\underbrace{a_k, a_k, ..., a_k}_{g \quad times}\}$$

then $\hat{A} = A_1 \cup A_2 \cup ... \cup A_k$ and $\hat{B} = B_1 \cup B_2 \cup ... \cup B_k$. By Lemma 3.3,

$$\hat{C} = \bigcup_{1 \le i, j \le k} (B_i \ominus A_j)$$

By Lemma 3.7, $B_i - A_j = \{(a_i - a_j)^{\vee g^2}\}, \quad 1 \le i, j \le k$; as a result,

$$\hat{C} = \{(a_i - a_j)^{\vee g^2} | a_i, a_j \in A, 1 \le i, j \le k\}$$

Meanwhile, $A \ominus A = \{a_i - a_j | a_i, a_j \in A, 1 \le i, j \le k\}$; this immediately leads to

$$\hat{C} = (A \ominus A)^{g^2}$$

□

Example 3.25. *Let* $A=\{1,2,3,4\}$ *;then*

$$A^2\ominus A^2=\left\{\begin{array}{cccccccc} 0, & 0, & -1, & -1, & -2, & -2, & -3, & -3, \\ 0, & 0, & -1, & -1, & -2, & -2, & -3, & -3, \\ 1, & 1, & 0, & 0, & -1, & -1, & -2, & -3, \\ 1, & 1, & 0, & 0, & -1, & -1, & -2, & -3, \\ 2, & 2, & 1, & 1, & 0, & 0, & -1, & -1, \\ 2, & 2, & 1, & 1, & 0, & 0, & -1, & -1, \\ 3, & 3, & 2, & 2, & 1, & 1, & 0, & 0, \\ 3, & 3, & 2, & 2, & 1, & 1, & 0, & 0 \end{array}\right\}$$
$$=\{-3^{\vee 4},-2^{\vee 8},-1^{\vee 12},0^{\vee 16},1^{\vee 12},2^{\vee 8},3^{\vee 4}\}$$

By (3.7),$A\ominus A=\{-3^{\vee 1},-2^{\vee 2},-1^{\vee 3},0^{\vee 4},1^{\vee 3},2^{\vee 2},3^{\vee 1}\}$*; it is sure* $\hat{B}\ominus\hat{A}=(A\ominus A)^{g^2}$.

Corollary 3.26. *Let* k *and* A *be defined as those in Theorem 3.8; then*

$$A^g\ominus A^g=\{(1-k)^{\vee g^2},(2-k)^{\vee 2g^2},...,-1^{\vee(k-1)g^2},0^{\vee kg^2},1^{\vee(k-1)g^2},2^{\vee(k-2)g^2},...,(k-2)^{\vee 2g^2},(k-1)^{\vee g^2}\} \tag{3.9}$$

For the set $\hat{C}$ *such that* $\hat{c}_{ij}=|c_{ij}|$*, where* $\hat{c}_{ij}\in\hat{C}$*, it follows*

$$\hat{C}=\{0^{\vee kg^2},1^{\vee 2(k-1)g^2},2^{\vee 2(k-2)g^2},...,s^{\vee 2(k-s)g^2},...,(k-2)^{\vee 4g^2},(k-1)^{\vee 2g^2}\} \tag{3.10}$$

where integer s *satisfies* $1\le s\le k-1$*.*

Proof. By Corollary 3.24, $A^g\ominus A^g=C^{g^2}$. Referring to (3.7) and (3.8) immediately results in (3.9) and (3.10). □

Corollary 3.27. *Let* A *be defined as that in Theorem 3.8; then*

$$(A\ominus A)^g=\{(1-k)^{\vee g},(2-k)^{\vee 2g},...,-1^{\vee(k-1)g},0^{\vee kg},1^{\vee(k-1)g},2^{\vee(k-2)g},...,(k-2)^{\vee 2g},(k-1)^{\vee g}\}$$

Proof. Referring to the new notations in section 2.2 and Corollary 3.16. □

Remark 3.4. Arranged in rows and columns, $(A\ominus A)^g$ is of the form

$$(A\ominus A)^g=\left\{\begin{array}{cccc} \underbrace{0,\ \cdots,\ 0,}_{g\ \ times} & \underbrace{-1,\ \cdots,\ -1,}_{g\ \ times} & \cdots\ \cdots & \underbrace{1-k,\ \cdots,\ 1-k,}_{g\ \ times} \\ \underbrace{1,\ \cdots,\ 1,}_{g\ \ times} & \underbrace{0,\ \cdots,\ 0,}_{g\ \ times} & \cdots\ \cdots & \underbrace{2-k,\ \cdots,\ 2-k,}_{g\ \ times} \\ \cdots & \cdots & \cdots\ \cdots & \cdots \\ \underbrace{k-1,\ \cdots,\ k-1,}_{g\ \ times} & \underbrace{k-2,\ \cdots,\ k-2,}_{g\ \ times} & \cdots\ \cdots & \underbrace{0,\ \cdots,\ 0,}_{g\ \ times} \end{array}\right\}$$

Theorem 3.28. *Given integers* a *,* $g>0$ *and* $N>0$*, assume* $A=\{a+1,a+2,...,a+N\}$ *and* $B=\{a+1,a+2,...,a+gN\}$*; then without considering the order of the elements, it holds*

$$(A\ominus A)^g \bmod N=(B\ominus B) \bmod N$$

Proof. By Corollary 3.27,

$$(A\ominus A)^g=\{(1-N)^{\vee g},(2-N)^{\vee 2g},...,-1^{\vee(N-1)g},0^{\vee Ng},1^{\vee(N-1)g},2^{\vee(N-2)g},...,(N-2)^{\vee 2g},(N-1)^{\vee g}\}$$

containing totally gN elements.

Hence it follows

$$(A \ominus A)^g \bmod N = (A \ominus A)^g$$

By Corollary 3.16,

$$B \ominus B = \{(1-gN)^{\vee 1}, (2-gN)^{\vee 2}, ..., -1^{\vee(gN-1)}, 0^{\vee gN}, 1^{\vee(gN-1)}, 2^{\vee(gN-2)}, ..., (gN-2)^{\vee 2}, (gN-1)^{\vee 1}\}$$

Now let $e_B \in B \ominus B$ be an arbitrary element such that $e_B \neq 0$; then it must be of the form $e_B = i \pm gN$ with $1 \leq i \leq N-1$. Note that , for $j = 1, 2, ..., g$, it holds

$$e_B \bmod N = i \pm gN \bmod N = i, \quad 1 \leq i \leq N-1$$

Hence it follows

$$(B \ominus B) \bmod N = \{(1-N)^{\vee g}, (2-N)^{\vee 2g}, ..., -1^{\vee(N-1)g}, 0^{\vee gN}, 1^{\vee(N-1)g}, 2^{\vee(N-2)}, ..., (N-2)^{\vee 2g}, (gN-1)^{\vee g}\}$$

establishing the theorem. □

4 Application in Integer Factorization

Given an odd semiprime $N = pq$, where p and q are odd integers such that $1 < p < q$. Assume p and q are bounded in two host intervals, say $I_p = [p_s, p_b]$ and $I_q = [q_s, q_b]$, respectively, where p_s, p_b, q_s, and q_b are odd positive integers satisfying $2 < p_s < p_b \leq \sqrt{N}$ and $\sqrt{N} \leq q_s < q_b$; finding out p in I_p or q in I_q surely factorizes N. The theorems and corollaries proven in the previous section show that elements hosting N's divisors can be concentrated in a set. This provides an opportunity to search the host elements in that set.

Let $A_p = [1, p_s - 1]$, $B_p = I_p$, $C_p = [p_b + 1, p_e]$, and $S_p = A_p \cup B_p \cup C_p$, where $p_e > p_b + 1$ is an integer; then

$$S \ominus S = \left\{ \begin{array}{cccccccccccc}
0, & -1, & -2, & \dots & -p_s, & \dots & \dots & -p_b, & \dots & \dots & -(p_e-3), & -(p_e-2), & -(p_e-1), \\
1, & 0, & -1, & \dots & \dots & -p_s, & \dots & \dots & -p_b, & \dots & -(p_e-4), & -(p_e-3), & -(p_e-2), \\
2, & 1, & 0, & \dots & \dots & \dots & \dots & \dots & \dots & v & \dots & -(p_e-4), & -(p_e-3), \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
p_s, & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & -p_b, & v \\
\dots & p_s, & \dots & \dots & \dots & \dots & -1, & \dots & \dots & \dots & \dots & v & -p_b, \\
\dots & \dots & \dots & \dots & \dots & \dots & 0, & -1, & \dots & \dots & \dots & \dots & \dots \\
p_b, & \dots & \dots & \dots & \dots & \dots & 1, & 0, & -1, & \dots & \dots & -p_s, & \dots \\
\dots & p_b, & \dots & \dots & \dots & \cdots & \dots & 1, & 0, & \dots & \dots & \dots & -p_s, \\
\dots & v & \dots & \dots & \dots & \dots & \dots & \dots & v & \dots & \dots & \dots & \dots \\
p_e-3, & p_e-4, & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0, & -1, & -2, \\
p_e-2, & p_e-3, & p_e-4, & \dots & p_b, & \dots & \dots & p_s, & \dots & \dots & 1, & 0, & -1, \\
p_e-1, & p_e-2, & p_e-3, & \dots & \dots & p_b, & \dots & \dots & p_s, & \dots & 2, & 1, & 0
\end{array} \right\}$$

By Remark 3.3, the elements in B_p repeatedly occur in $S \ominus S$ and a bigger p_e will increase the repeated times. This surely provides a way to enhance the chance to find out an objective element. We next investigate two typical cases: $p_e = N$ and $p_e = gN$, where $g \geq 1$ is an integer.

4.1 Case $\mathbf{P_e = N}$

The case $p_e = N$ yields

$$S \ominus S = \begin{Bmatrix} 0, & -1, & -2, & \cdots & -p_s, & \cdots & \cdots & -p_b, & \cdots & \cdots & -(N-3), & -(N-2), & -(N-1), \\ 1, & 0, & -1, & \cdots & \cdots & -p_s, & \cdots & \cdots & -p_b, & \cdots & -(N-4), & -(N-3), & -(N-2), \\ 2, & 1, & 0, & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & -(N-4), & -(N-3), \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & -p_s, & \cdots & \cdots & \cdots & \cdots & \cdots \\ p_s, & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & -p_b, & \cdots \\ \cdots & p_s, & \cdots & \cdots & \cdots & \cdots & -1, & \cdots & \cdots & \cdots & \cdots & \cdots & -p_b, \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0, & -1, & \cdots & \cdots & \cdots & \cdots & \cdots \\ p_b, & \cdots & \cdots & \cdots & \cdots & \cdots & 1, & 0, & -1, & \cdots & \cdots & -p_s, & \cdots \\ \cdots & p_b, & \cdots & \cdots & \cdots & \cdots & \cdots & 1, & 0, & \cdots & \cdots & \cdots & -p_s, \\ \cdots & \cdots & \cdots & \cdots & \cdots & p_s, & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ N-3, & N-4, & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0, & -1, & -2, \\ N-2, & N-3, & N-4, & \cdots & p_b, & \cdots & \cdots & p_s, & \cdots & \cdots & 1, & 0, & -1, \\ N-1, & N-2, & N-3, & \cdots & \cdots & p_b, & \cdots & \cdots & p_s, & \cdots & 2, & 1, & 0 \end{Bmatrix} \tag{4.1}$$

or

$$\hat{S}_p = \{0^{\vee N}, 1^{\vee 2(N-1)}, ..., j^{\vee 2(N-j)}, ..., (p_s-1)^{\vee 2(N-p_s+1)}, {p_s}^{\vee 2(N-p_s)}, ..., (p_s+j)^{\vee 2(N-p_s-j)}, ..., (N-2)^{\vee 4}, (N-1)^{\vee 2}\}$$

It hence follows in $\hat{S}_p$

$$m_p = 2(N-p_s-p), m_{2p} = 2(N-p_s-2p), ..., m_{\alpha p} = 2(N-p_s-\alpha p), ..., m_{(q-1)p} = 2(N-p_s-(q-1)p)$$

where α is an integer satisfying $1 \leq \alpha \leq q-1$.

The elements hosting divisor p are distributed sparsely in $\hat{S}_p$, occurring every p elements from the first occurrence . Their total number is

$$n_p = 2(N-p_s-p) + 2(N-p_s-2p) + ... + 2(N-p_s-\alpha p) + ... + 2(N-p_s-(q-1)p) = (q-1)N$$

Note that, $p_e = N$ means $\hat{S}_p$ also contains $q, 2q, 3q$,...,$(p-1)q$. They occur every q elements from the first occurrence and their total number is given by

$$n_q = (p-1)N$$

Therefore, the total number of the elements hosting N's divisors in $\hat{S}_p$ is given by

$$n_d = n_p + n_q = (p+q-2)N$$

For example, taking $N = 35$ leads to p =5 and q =7. Direct calculation shows $\hat{S}_{35}$ has sixty elements taking value 5, fifty elements taking value 10, forty elements taking value 15, thirty elements taking value 20, twenty elements taking value 25, and ten elements taking value 30, totally 210 elements containing divisor 5. It also has fifty six elements taking value 7, forty two elements taking value 14, twenty

eight elements taking value 21, and fourteen elements taking value 28, totally 140 ones.

Now seen in (4.1), the negative and positive elements are separated by the N zeros and look like two triangles, each of which contain the same number of the elements hosting N's divisors. Seen in the lower triangle, there is a band bordered with the repeated elements of p_s and p_b respectively, as illustrated in Figure 2. Since $p_s \leq p \leq p_b$, the repeated elements of p are contained in the band. So that the band is called a p-band. Meanwhile the triangle lower the p-band contains all the elements of αp with integer $\alpha > 1$, and all the elements of βq with integer $\beta \geq 1$. Hence the triangle is called a *pq*-triangle.

$$
S \ominus S = \left\{ \begin{array}{ccccccccccccc}
0, & -1, & -2, & \cdots & -p_s, & \cdots & \cdots & -p_b, & \cdots & \cdots & -(N-3), & -(N-2), & -(N-1), \\
1, & 0, & -1, & \cdots & \cdots & -p_s, & \cdots & \cdots & -p_b, & \cdots & -(N-4), & -(N-3), & -(N-2), \\
2, & 1, & 0, & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & -(N-4), & -(N-3), \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & -p_s, & \cdots & \cdots & \cdots & \cdots & \cdots \\
p_s, & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & -p_b, & \cdots \\
\cdots & p_s, & \cdots & \cdots & \cdots & \cdots & -1, & \cdots & \cdots & \cdots & \cdots & \cdots & -p_b, \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0, & -1, & \cdots & \cdots & \cdots & \cdots & \cdots \\
p_b, & \cdots & \cdots & \cdots & \cdots & \cdots & 1, & 0, & -1, & \cdots & \cdots & -p_s, & \cdots \\
\cdots & p_b, & \cdots & \cdots & \cdots & \cdots & \cdots & 1, & 0, & \cdots & \cdots & \cdots & -p_s, \\
\cdots & \cdots & \cdots & \cdots & \cdots & p_s, & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
N-3, & N-4, & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0, & -1, & -2, \\
N-2, & N-3, & N-4, & \cdots & p_b, & \cdots & \cdots & p_s, & \cdots & \cdots & 1, & 0, & -1, \\
N-1, & N-2, & N-3, & \cdots & \cdots & p_b, & \cdots & \cdots & p_s, & \cdots & 2, & 1, & 0
\end{array} \right\}
$$

Figure 2: p-band and *pq*-triangle in $\hat{S}_p$

The number of the elements in the p-band is

$$n_{p-band} = \frac{1}{2}(2N - p_b - p_s)(p_b - p_s + 1)$$

and that in the *pq*-triangle is

$$n_{pq-\Delta} = \frac{1}{2}(N - p_b - 1)(N - p_b)$$

As a result, the total number of the elements in both the p-band and the *pq*-triangle all together is calculated by

$$n_{both} = \frac{1}{2}(N - p_s)(N - p_s + 1)$$

On the other hand, the number of the repeated elements of p in the p-band is

$$n^p_{p-band} = N - p - p_s$$

hence the number of the elements hosting N's divisors in the *pq*-triangle is

$$n^d_{pq-\Delta} = (p+q-2)N - N - p_s - p = (p-3)N + (q-p)N - p_s$$

Now let

$$pq\text{-both} = p\text{-band} \cup pq\text{-triangle}$$

We check the density or the concentration of the elements hosting a divisor of N in the p-band, *pq*-triangle, and *pq*-both. This can done by picking randomly an element in the three areas respectively and seeing the probability of successfully obtaining a divisor.

Since

$$P^p_{p-band} = \frac{n^p_{p-band}}{n_{p-band}} = \frac{2(N-p-p_s)}{(2N-p_b-p_s)(p_b-p_s+1)}$$

$$P^d_{pq-\Delta} = \frac{n^d_{pq-\Delta}}{n_{pq-\Delta}} = \frac{2((p+q-2)N-N-p_s-p)}{(N-p_b-1)(N-p_b)}$$

and

$$P^d_{both} = \frac{n_d}{n_{both}} = \frac{2(p+q-2)N}{(N-p_s)(N-p_s+1)}$$

direct calculations show

$$\frac{P^d_{pq-\Delta}}{P^p_{p-band}} = (p_b-p_s+1)(1+\frac{p_b}{N-\ p_b})(1+\frac{N-p_s+1}{N-\ p_b-1})(1+\frac{p+q}{N-p-\ p_s}) > 2(p_b-p_s+1) \tag{4.2}$$

and

$$\frac{P^d_{both}}{P^d_{pq-\Delta}} = \frac{(N-p_b)(N-p_b-1)}{2(N-p_s)(N-p_s+1)}(1+\frac{N+p_s+p}{(p+q-2)N-N-p_s-p}) \tag{4.3}$$

Because

$$q > p > p_s \Rightarrow \frac{N+p_s+p}{(p+q-2)N-N-p_s-p} < \frac{N+2p}{2p(N-1)-3N}$$
$$\Rightarrow 1+\frac{N+p_s+p}{(p+q-2)N-N-p_s-p} < 1+\frac{N+2p}{2p(N-1)-3N} = \frac{2(p-1)N}{(2p-3)N-2p}$$

and

$$\frac{2(p-1)N}{(2p-3)N-2p} = \frac{2(p-1)N}{(2p-2)N-N-2p} = \frac{2}{2-\frac{N+2p}{pN-N}} = \frac{2}{2-\frac{1}{\frac{pN+2p}{N+2p}-1}} < 2$$

it follows with (4.3)

$$\frac{P^d_{both}}{P^d_{pq-\Delta}} < \frac{(N-p_b)(N-p_b-1)}{(N-p_s)(N-p_s+1)} < 1 \tag{4.4}$$

The inequalities (4.4) and (4.2) indicate that the elements hosting N's divisors are more densely distributed in the *pq*-triangle. In another word, the concentration of the elements hosting N's divisors in the *pq*-triangle is bigger than that either in the p-band or in the *pq*-both.

4.2 Case $\mathbf{p_e = gN}$

Denote $\Xi = [1, gN]$; then

$$\Xi\ominus\Xi = \{(1-gN)^{\vee 1}, (2-gN)^{\vee 2}, ..., -1^{\vee(gN-1)}, 0^{\vee gN}, 1^{\vee(gN-1)}, 2^{\vee(gN-2)}, ..., (gN-2)^{\vee 2}, (gN-1)^{\vee 1}\}$$

containing $(q-1)gN$ elements hosting divisor p and $(p-1)gN$ elements hosting divisor q. Since each element except 0 is of the form $i \pm jN$with $1 \leq i \leq N-1$and $0 \leq j \leq g$, the elements hosting divisor p occur every p elements from the first occurrence and those hosting divisor q occur every q elements from the first occurrence.

Like that of (4.1), $\Xi \ominus \Xi$ can be arranged in rows and columns by

$$\Xi\ominus\Xi = \left\{\begin{array}{cccccccccccccc}
0, & -1, & -2, & \cdots & -p, & \cdots & \cdots & -2p, & \cdots & \cdots & -(gN-3), & -(gN-2), & -(gN-1), \\
1, & 0, & -1, & \cdots & \cdots & -p, & \cdots & \cdots & -2p, & \cdots & \cdots & -(gN-3), & -(gN-2), \\
2, & 1, & 0, & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & -(gN-3), \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & -p, & \cdots & \cdots & \cdots & \cdots & \cdots \\
p, & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & -2p, & \cdots \\
\cdots & p, & \cdots & \cdots & \cdots & \cdots & -1, & \cdots & \cdots & \cdots & \cdots & \cdots & -2p, \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0, & -1, & \cdots & \cdots & \cdots & \cdots & \cdots \\
2p, & \cdots & \cdots & \cdots & \cdots & \cdots & 1, & 0, & -1, & \cdots & \cdots & -p, & \cdots \\
\cdots & 2p, & \cdots & \cdots & \cdots & \cdots & \cdots & 1, & 0, & \cdots & \cdots & \cdots & -p, \\
\cdots & \cdots & \cdots & \cdots & \cdots & p, & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
gN-3, & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0, & -1, & -2, \\
gN-2, & gN-3, & \cdots & \cdots & \cdots & \cdots & \cdots & p, & \cdots & \cdots & 1, & 0, & -1, \\
gN-1, & gN-2, & gN-3, & \cdots & \cdots & 2p, & \cdots & \cdots & p, & \cdots & 2, & 1, & 0
\end{array}\right\}$$

Seen from the point-view of rows and columns, from the first occurrence, the elements hosting divisor p occur every p rows or columns while the elements hosting divisor q occur every q rows or columns, all sparsely distributed in $\Xi \ominus \Xi$.
Now consider $\Xi \ominus \Xi \bmod N$. By Theorem 3.28,

$$(S \ominus S)^g = \Xi \ominus \Xi(\mathrm{mod} N)(S)$$

As a result, the case $p_e = gN$ is turned into the repeated case of $p_e = N$. Arranged in rows and columns, $(S \ominus S)^g$ is of the form described with Figure 3.

There are surely a p^g-band, a (pq)^g-triangle and a (pq)^g-both like those in $S \ominus S$. Similarly, the elements hosting$N$'s divisors are denser in the (pq)^g-triangle than those in the other two zones, the p^g-band and (pq)^g-both.

4.3 Elements in pq-triangle

Denote the pq-triangle with symbol Δ_{pq}. By definition, Δ_{pq} can be geometrically considered to be an isosceles right triangle. Each of its two legs is formed by the

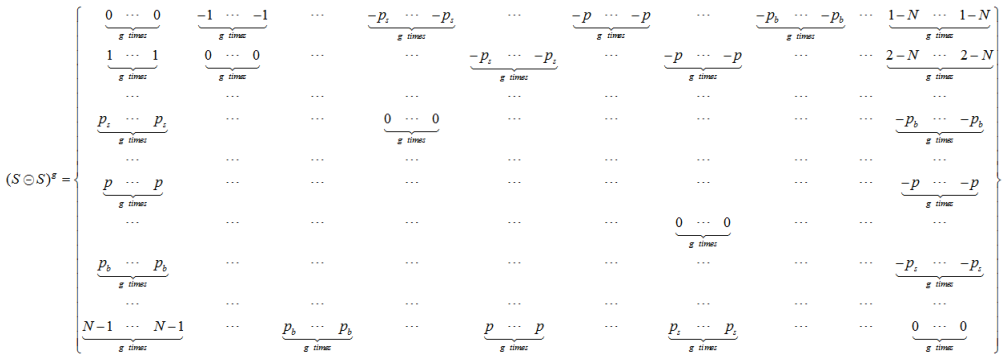

Figure 3: $(S \ominus S)^g$ in the form of rows and columns

elements $p_b+1, ..., p_b+j, ...,$ and $N-1$ while its hypotenuse is composed of $N-p_b-1$ elements with the same value p_b+1. Using X and Y to express the indices of the row and the column of Δ_{pq} respectively, it follows

$$1 \leq X \leq N - p_b - 1 \text{ and } 1 \leq Y \leq X$$

and the three borders are lattices such that

$$\text{line } Y = 1, \text{ line } X = N - p_b - 1 \text{ and } Y = X$$

The element $\omega_{X,Y}$ at row X and column Y is calculated by

$$\omega_{X,Y} = p_b + 1 + X - Y$$

4.4 Elements in (pq)^g-triangle

Denote the $(pq)^g$-triangle by symbol T^g_{pq}; then

$$T^g_{pq} = \{(p_b+1)^{\vee g(N-p_b-1)}, ..., e = (p_b+j)^{\vee g(N-p_b-j)}, ..., (N-2)^{\vee 2g}, (N-1)^{\vee g}\}$$

Arranged in rows and columns, it is of the form

$$T^g_{pq} = \left\{ \begin{array}{lll} \underbrace{p_b+1 \quad \cdots \quad p_b+1}_{g \quad times}, & & \\ \cdots & \cdots & \\ \underbrace{e \quad \cdots \quad e}_{g \quad times}, & \cdots \quad \underbrace{p_b+1 \quad \cdots \quad p_b+1}_{g \quad times}, & \\ \cdots & \cdots \quad \cdots & \cdots \\ \underbrace{N-1 \quad \cdots \quad N-1}_{g \quad times}, & \cdots \quad \underbrace{e \quad \cdots \quad e}_{g \quad times}, & \cdots \quad \underbrace{p_b+1 \quad \cdots \quad p_b+1}_{g \quad times}, \end{array} \right\}$$

T_{pq}^{g} is geometrically seen to be a right trapezium with one side composed of $(N - p_b - 1)g$ elements of $p_b + 1$. Take on each row one $p_b + 1$ to form the following right triangle Δ_{pq}^{g}:

row 1: $d_{1,1} = p_b + 1$;

row 2: $\underbrace{d_{2,1} = d_{2,2} = ... = d_{2,g} = p_b + 2}_{g \quad items}, d_{2,g+1} = p_b + 1$;

row 3:

$$\underbrace{d_{3,1} = d_{3,2} = ... = d_{3,g} = p_b + 3}_{g \quad items}, \underbrace{d_{3,g+1} = ... = d_{3,2g} = p_b + 3 - 1}_{g \quad items},$$
$$d_{3,2g+1} = p_b + 3 - 2$$

row 4:

$$\underbrace{d_{4,1} = ... = d_{4,g} = p_b + 4}_{g \quad items}, \underbrace{d_{4,g+1} = ... = d_{4,2g} = p_b + 4 - 1}_{g \quad items},$$
$$\underbrace{d_{4,2g+1} = ... = d_{4,3g} = p_b + 4 - 2}_{g \quad items}, d_{4,3g+1} = p_b + 4 - 3$$

row k:

$$\underbrace{d_{k,1} = ... = d_{k,g} = p_b + k}_{g \quad items}, ..., \underbrace{d_{k,(j-1)g+1} = ... = d_{k,jg} = p_b + k - (j-1)}_{g \quad items}, ...,$$
$$\underbrace{d_{k,(k-2)g} = ... = d_{k,(k-1)g} = p_b + 2}_{g \quad items}, d_{4,(k-1)g+1} = p_b + k - (k-1) = p_b + 1$$

where $1 \leq k \leq N - p_b - 1$ and $1 \leq j \leq k - 1$.

Still using X and Y to express the indices of the row and the column respectively, it follows

$$1 \leq X \leq N - p_b - 1, 1 \leq Y \leq (X-1)g + 1$$

and the three borders of Δ_{pq}^{g} are lattices corresponding to

$$\text{line } Y = 1, \text{ line } X = N - p_b - 1, \text{ and line } Y = (X-1)g + 1.$$

The element $\Omega_{X,Y}$ at row X and column $Y$is

$$\Omega_{X,Y} = p_b + X - \left\lfloor \frac{Y-1}{g} \right\rfloor \tag{4.5}$$

By the way, it is sure that the concentration of the elements hosting N's divisors is bigger in Δ_{pq}^{g} than that in T_{pq}^{g} because the total number of the elements in Δ_{pq}^{g} is less than that in T_{pq}^{g}.

4.5 Random-walk Approach to Find a Divisor-host

Now that Δ_{pq} and Δ_{pq}^{g} has the most concentration of the elements hosting N's divisors, it is a natural choice to search N's divisors in either of them. Once one of the host elements, say e, is found, d =gcd(e, N) is surely the divisor of N. Theoretically there are many approaches for such searching. Here we introduce the approach of using a two-dimensional simple random walk to perform the search.

Our random walk is obviously the one within a bounded domain. As seen in literatures such as [11], [12], and [13], the start point, restart point, and walking-step are primarily necessary for the random walk within a bounded domain.

By the recurrent property and the distribution property of the two-dimensional simple random walk, the start point, say (X_0, Y_0), is better to set near where the elements hosting N's divisors locate. Since those host elements are unknown before one of them is found, an initial start point can be chosen by a rough estimation. Note that $p \le \sqrt{N} \le q \Rightarrow ip \le i\sqrt{N} \le iq$ for an arbitrary positive integer i , p is out of T_{Δ}^{g}, and $\left\lfloor \sqrt{N} \right\rfloor$ is the biggest i such that $i\sqrt{N} \le N$; X_0 can be chosen by

$$X_0 = \alpha \left\lfloor \sqrt{N} \right\rfloor$$

where $1 < \alpha \le \left\lfloor \sqrt{N} \right\rfloor$ is an integer.

Then Y_0 is chosen by $Y_0 = X_0$ if the walk is in Δ_{pq}; otherwise $Y_0 = gX_0$.

If the random walk goes out of the zone, Δ_{pq} or Δ_{pq}^{g}, it is forced to restart a next round. The restart point , say (X_{rst}, Y_{rst}), is better to choose like the choice of (X_0, Y_0) because it ensures the restart point near the elements hosting N's divisors.

For a walk in Δ_{pq}, its walking step δ_x in X-direction and step δ_y are set to be the same one though they can be set to different ones. For a walk in Δ_{pq}^{g}, δ_x is different from δ_y because each distinct lattice along the Y-direction is wrapped by g times, and the total number of the lattices along the Y-direction is almost g times of that along X-direction.

Finally, the random walk will be forced to stop if it walks too many steps, say B steps, without finding the objective element.

After all the preliminary settings done, the random-walk algorithm is designed to find a divisor of a composite integer N as follows.

Remark 4.1. The Algorithm 1 is designed for the random walk in Δ_{pq}^{g}. It can also applied on Δ_{pq} by taking g =1 . The parameter p_b can be chosen around $\sqrt{N}$ while δ_x , δ_y are chosen tentatively. In the algorithm, the subroutine aRandStep(X ,Y , δ_x , δ_y) is to calculate the next position of a random move from (X, Y) by steps δ_x and δ_y, OutofBorder(X, Y) is to test whether (X, Y) is out of the border, and SetStart($\sqrt{N}$) is to set the start point that is randomly chosen near the elements hosting N's divisors. The subroutine SetStart perform the following calculations.

Algorithm 1 Random-walk Algorithm to Factorize Integer

Input: N, p_b,g,δ_x,δ_y,B;
Step 1. (X, Y) =SetStart($\sqrt{N}$);
Step 2. Initialize counter = 0 and f =1;
Step 3. **Loop** while $f = 1$ and counter $<B$;
Calculate $\omega = p_b + X - \left\lfloor \frac{Y-1}{g} \right\rfloor$ and f = gcd(N, ω);
if f >1 **then** break loop; **endif**;
(X, Y)=aRandStep(X ,Y , δ_x , δ_y);
if OutofBorder(X, Y) **then** (X ,Y)= SetStart($\sqrt{N}$); **endIf**;
counter=counter+1;
endloop
Step 4.**if** f >1 **then** Output f and counter;
else Declare failure of search; **endif**

Algorithm 2 Subroutine SetStart

Input: $\sqrt{N}$;
Step 1. Select randomly an integer $\alpha \in [2, \left\lfloor \sqrt{N} \right\rfloor]$;
Step 2. Calculate $X = \alpha \left\lfloor \sqrt{N} \right\rfloor$ and $Y = gX$;
Output: X, Y;

4.5.1 Numerical Experiments

With Maple software, we programmed a program that factorized integers with random walk in Δ_{pq} according to the designed algorithm. The source codes of the program are list in the appendix section. We take randomly semiprimes that contain 5 to 10 digits to do our numerical experiments. The results are shown in Table 1. In the table, the column 'Failure?' records if there is a failure in the experiments. Readers can see the experimental data in the appendix section.

Table 1: Records of Numerical Experiments

Semiprime N	Digits of N	Number of Experiments	Min Searching Steps	Max Searching Steps	Failure?
49901	5	5	26	271	Yes
567191	6	5	78	436	Yes
2425789	7	7	48	955	Yes
75506467	8	5	2105	5574	Yes
826522877	9	5	474	27480	Yes
1231065553	10	5	1108	34289	Yes

It should be pointed out that, the random-walk method of factoring integer exhibits randomization. One experiment is hardly identical to the other one even with the same input arguments. That is the essence of the random algorithm, as claimed in [3].

5 Conclusion and Future Work

Densification of the objective elements surely enriches the abundance of witnesses. The research in this paper shows the Cartesian subtraction can realize densification of certain elements in a countable set because the operation can make a set without repeated elements be a set with repeated elements. Our experiments that apply the two dimensional simple random walk to factorize composite integers show that densification and the random algorithm are trustable.

Nevertheless, we still have work to do related with this paper. For example, how to set a proper start point or a restart point and how to choose proper parameters δ_x and δ_y for a random walk in Δ_{pq}^{g} still need investigating. In addition, we need to promote the efficiency of the random walk algorithm so as for the algorithm to be a practical one. These remain our future work. Hope more young people to join us.

References

[1] A W Wanambisi, S Aywa, C Maende and G Muchiri Muketha. *Advances in Composite Integer Factorization*, Methematical theory and Modeling, 13(2013), No.2, 86-90

[2] DLMF. NIST Digital Library of Mathematical Functions. 2023, accessed at: http://dlmf.nist.gov/27.19

[3] R M Karp.*An introduction to randomized Algorithms*, Discrete Applied Mathematics, 34(1991), 165-201

[4] S Chakraborty, K S Meel, M Y Vardi. *A Scalable and Nearly Uniform Generator of SAT Witnesses*. Lecture Notes in Computer Science, 8044(2013). https://doi.org/10.1007/978-3-642-39799-8_40

[5] Y Zhao, X Jin, G Ciardo. *A Symbolic Algorithm for Shortest EG Witness Generation*, 2011 Fifth International Conference on Theoretical Aspects of Software Engineering, Xi'an, China, 2011, 68-75, doi: 10.1109/TASE.2011.35

[6] X Luo, S Liang, L Zheng and et.al.*Incremental Witness Generation for Branching-Time Logic CTL**,IEEE Transactions on Reliability, 71(2022), No. 2, 933-950. https://doi.org/10.1109/TR.2022.3146200.

[7] F Besson, T Jensen, T Turpin.*Small Witnesses for Abstract Interpretation-Based Proofs*,Lecture Notes in Computer Science, 4421(2007). https://doi.org/10.1007/978-3-540-71316-6_19

[8] K Meeks. *Randomised Enumeration of Small Witnesses Using a Decision Oracle*, Algorithmica, 81(2019), 519–540.. https://doi.org/10.1007/s00453-018-0404-y

[9] H Dell, J Lapinskas, K Meeks. *Approximately counting and sampling small witnesses using a colourful decision oracle*, arXiv:1907.04826v2 [cs.DS]. 2022.https://doi.org/10.48550/arXiv.1907.04826

[10] Eric W Weisstein. CRC Concise Encyclopedia of Mathematics , Chapman & Hall/CRC, 2003. page: 2960,2670

[11] A Mazzolo1. *Properties of diffusive random walks in bounded domains*, EPL, 68(2004), No.3,350-355

[12] H Ciftci, M Cakmak.*The confined random walks in two-dimensional bounded domain*, EPL, 87(2009), 60003. https://doi.org/10.1209/0295-5075/87/60003

[13] M Basu, P K Mohanty.*Two-dimensional random walk in a bounded domain*,EPL 90(2010), 50005. https://arxiv.org/abs/0910.5885v2

Appendix

A Maple Source Codes and Experimental Cases

A.1 Maple Source Codes

```
# Subrountie:- aRandStep2D
    aRandStep2D := proc(X0, Y0, dx, dy)
      local X, Y, P, R;
      P := Array(1 .. 2);
      R := rand(1 .. 8)();
      if R = 1 then X := X0 - dx; Y := Y0 + dy; end if;
      if R = 2 then X := X0; Y := Y0 + dy; end if;
      if R = 3 then X := X0 + dx; Y := Y0 + dy; end if;
      if R = 4 then X := X0 - dx; Y := Y0; end if;
      if R = 5 then X := X0 + dx; Y := Y0; end if;
      if R = 6 then X := X0 - dx; Y := Y0 - dy; end if;
      if R = 7 then X := X0; Y := Y0 - dy; end if;
      if R = 8 then X := X0 + dx; Y := Y0 - dy; end if;
      P[1] := X; P[2] := Y;
      return P;
    end proc
    # Subrountie:- SetStart
    SetStart := proc(b)
      local alpha, R, P;
      P:= Array(1 .. 2);
      alpha:= rand(1 .. b)();
      P[1] := alpha*b;
      P[2] := alpha*b;
      return P;
    end proc
    # MainRountie:- RandomFactTpq
    RandomFactTpq := proc(N, pb, dx, dy)
      local alpha, X, Y, f, P, counter, B, n, T;
      P := Array(1 .. 2);
```

```
    counter := 0; f := 1;
    B := floor(evalf(sqrt(N))); #Set maximal searching steps
    T := floor(evalf(sqrt(N))); #For SetStart's use
    P := SetStart(T);
    X := P[1]; Y := P[2];
    while f = 1 and counter <B do #loop
      n:= pb - X - Y;
      f:= gcd(N, n);
      if f ¿ 1 and f ¡ N then break; end if;
      P := aRandStep2D(X, Y, dx, dy); #A random move
      X := P[1]; Y := P[2];
      if X ¡ 1 or Y ¡ 1 or N - pb - 1 ¡ X or X ¡= Y then
        P := SetStart(T); # Restart when out of borders
        X := P[1]; Y := P[2];
      end if;
    counter := counter + 1; #Counting the searched steps
    end do;
    if f ¿ 1 then print(Find at point (X, Y), found divisor = f,searching steps =
counter);
    else print(This*time*finds*no*result, test*again!); end if;
  end proc
```

A.2 Experimental Cases

The following experimental cases are run in Maple with the programs list in the previous section. The original data are reserved at the webpage:
https://www.mapleprimes.com/DocumentFiles/221856_post/wxbRandWalkTpqNew4.pdf

```
RandomFactTpq(49901, 150, 1, 1);
  Find at point (2230, 2229), found divisor = 139, searching steps = 77
RandomFactTpq(49901, 150, 1, 1);
  Find at point (17173, 17171), found divisor = 139, searching steps = 211
RandomFactTpq(49901, 150, 1, 1);
  Find at point (27875, 27875), found divisor = 139, searching steps = 141
RandomFactTpq(49901, 150, 1, 1);
  Find at point (16948, 16948), found divisor = 359, searching steps = 26
RandomFactTpq(49901, 150, 1, 1);
  This time finds no result, test factorial(again)
RandomFactTpq(567191, 700, 1, 1);
  Find at point (51960, 51955), found divisor = 983, searching steps = 436
RandomFactTpq(567191, 700, 1, 1);
  Find at point (405118, 405113), found divisor = 577, searching steps = 78
```

RandomFactTpq(567191, 700, 1, 1);
Find at point (360687, 360686), found divisor = 577, searching steps = 243
RandomFactTpq(567191, 700, 1, 1);
Find at point (480414, 480414), found divisor = 577, searching steps = 157
RandomFactTpq(567191, 700, 1, 1);
This time finds no result, test factorial(again)
RandomFactTpq(2425789, 1500, 2, 2);
Find at point (351976, 351828), found divisor = 1291, searching steps = 955
RandomFactTpq(2425789, 1500, 2, 2);
Find at point (2186028, 2186026), found divisor = 1879, searching steps = 496
RandomFactTpq(2425789, 1500, 2, 2);
Find at point (926471, 926323), found divisor = 1291, searching steps = 859
RandomFactTpq(2425789, 1500, 2, 2);
Find at point (2158020, 2158002), found divisor = 1291, searching steps = 177
RandomFactTpq(2425789, 1500, 2, 2);
Find at point (1077444, 1077444), found divisor = 1291, searching steps = 48
RandomFactTpq(75506467, 8500, 3, 3);
Find at point (53559017, 53559005), found divisor = 9739, searching steps = 2105
RandomFactTpq(75506467, 8500, 3, 3);
Find at point (58624683, 58624683), found divisor = 7753, searching steps = 3959
RandomFactTpq(75506467, 8500, 3, 3);
Find at point (27318333, 27317805), found divisor = 7753, searching steps = 5072
RandomFactTpq(75506467, 8500, 3, 3);
Find at point (16083339, 16083339), found divisor = 9739, searching steps = 5574
RandomFactTpq(75506467, 8500, 3, 3);
This time finds no result, test factorial(again)
RandomFactTpq(826522877, 28000, 7, 7);
Find at point (693828366, 693828366), found divisor = 35323, searching steps = 22337
RandomFactTpq(826522877, 28000, 7, 7);
Find at point (152945149, 152944708), found divisor = 35323, searching steps = 20818
RandomFactTpq(826522877, 28000, 7, 7);
Find at point (624802626, 624802171), found divisor = 23399, searching steps = 27480
RandomFactTpq(826522877, 28000, 7, 7);

Find at point (144233740, 144233733), found divisor = 23399, searching steps = 474

RandomFactTpq(826522877, 28000, 7, 7);

This time finds no result, test factorial(again)

RandomFactTpq(1231065553, 35000, 11, 11);

Find at point (495624803, 495624528), found divisor = 30853, searching steps = 16533

RandomFactTpq(1231065553, 35000, 11, 11);

Find at point (735472732, 735472732), found divisor = 39901, searching steps = 3899

RandomFactTpq(1231065553, 35000, 11, 11);

Find at point (432329780, 432329692), found divisor = 30853, searching steps = 1108

RandomFactTpq(1231065553, 35000, 11, 11);

Find at point (972689178, 972689178), found divisor = 30853, searching steps = 34389