Parabola Volume 59, Issue 1 (2023)

Is subtraction really the inverse of addition?

A careful look at the invertibility of operations

Rizky Reza Fauzi[1], **Steven**[2], and **Jonathan Hoseana**[3]

1 Introduction

Many school-level arithmetic books [3, 6, 8, 10, 12], when discussing the concept of subtraction, employ the sentence

$$\text{“Subtraction is the inverse of addition.”} \tag{1}$$

Certainly, as explained in most of these books, this sentence is meant to be a shorter and easier-to-memorise version of

$$\text{“Subtraction \textit{by a number} is the inverse of addition \textit{by the same number}.”} \tag{2}$$

However, when students end up memorising the sentence (1) without sufficient awareness that it actually means (2), concerns arise. Indeed, this could lead them to an imperfect understanding of *inverse functions* in their future study of higher mathematics, since the sentence (1), in itself, uses the word *inverse* in an improper way.

But why exactly is the use of the word *inverse* in the sentence (1) improper? That is, why is subtraction actually *not* the inverse of addition? In this article, we aim to answer this question carefully. Our first step is to articulate what kind of mathematical objects are addition and subtraction. This starting point, as we shall see, will subsequently lead to an interesting mathematical discussion.

2 Operations and their invertibility

Both addition and subtraction are *operations* on the set of real numbers. An operation is a special type of *function*, whose standard definition we now recall [1, 5].

[1]Rizky Reza Fauzi is a researcher at the Centre for Mathematics and Society, Department of Mathematics, Parahyangan Catholic University, Bandung, Indonesia. (`rrfauzi@unpar.ac.id`)

[2]Steven is a Ph.D. candidate at the School of Mathematics and Statistics, University of Sheffield, Hicks Building, Sheffield, United Kingdom. (`s-1@sheffield.ac.uk`)

[3]Jonathan Hoseana is the head of the Centre for Mathematics and Society, Department of Mathematics, Parahyangan Catholic University, Bandung, Indonesia. (`j.hoseana@unpar.ac.id`)

Definition 1. A *function* f from a set A to a set B, written $f : A \to B$, is a mathematical object which associates *every* element $x \in A$ to a *unique* element $f(x) \in B$. In symbols, we write

$$f : A \to B, \quad x \mapsto f(x) .$$

We refer to $f(x)$ as the *image* of x under f, and x as a[4] *preimage* of $f(x)$ under f. The sets A and B are called the *domain* and the *codomain*, respectively, of f.

For example, the function

$$f : \{-2, 0, 2\} \to \{0, 1, 4\}, \quad x \mapsto x^2 \tag{3}$$

associates every element of its domain to its square:

$$f(-2) = (-2)^2 = 4, \quad f(0) = 0^2 = 0, \quad \text{and} \quad f(2) = 2^2 = 4 .$$

The fact that $f(-2) = 4$ means that the image of -2 under f is 4, and that a preimage of 4 under f is -2. Another preimage of 4 under f is 2, since $f(2) = 4$.

The standard definition of an operation now follows [2, 4, 5].

Definition 2. An *operation* on a set A is a function from the set $A \times A$ of all ordered pairs of elements of A, to the set A.

For example, the function

$$g : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, \quad (a, b) \mapsto \max\{a, b\}$$

is an operation on the set $\mathbb{R}$ of real numbers, which associates every ordered pair (a, b) of real numbers to the maximum $\max\{a, b\}$ of its components: a if $a \geqslant b$, and b if $a < b$. Thus,

$$g(2, 0) = \max\{2, 0\} = 2\,, \quad g(-2, 1) = \max\{-2, 1\} = 1\,, \quad \text{and} \quad g(0, 0) = \max\{0, 0\} = 0\,.$$

Now, addition and subtraction of real numbers are the functions

$$+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}\,, \quad (a, b) \mapsto a + b\,, \qquad \text{and} \qquad - : \mathbb{R} \times \mathbb{R} \to \mathbb{R}\,, \quad (a, b) \mapsto a - b\,,$$

respectively; they associate every ordered pair of real numbers to the sum and the difference, respectively, of its components. Therefore, being a function, whether an operation has an inverse[5] is determined by its injectivity, surjectivity, and, ultimately, bijectivity [1, 2, 4, 5].

---

[4]Notice that we use the indefinite article "a" here, rather than the definite article "the", to indicate that a codomain element need not have a unique preimage.

[5]Given an operation $\oplus : A \times A \to A$ and an element $a \in A$, notice the difference that exists between *the inverse of the operation* $\oplus$, *the inverse of the element* a *under the operation* $\oplus$, and *the inverses of the actions* $x \mapsto a \oplus x$ *and* $x \mapsto x \oplus a$ *of the element* a *on* A. Assuming existence, these are, respectively, a function from A to $A \times A$, an element of A, and functions from A to A.

Definition 3. A function is *injective* if every element of its codomain has at most one preimage, is *surjective* if every element of its codomain has at least one preimage, and is *bijective* if it is both injective and surjective, i.e., if every element of its codomain has exactly one preimage.

For example, the function f given by (3) is not injective since, as we have seen, the element 4 of its codomain has two distinct preimages: 2 and -2. It is also not surjective, since the element 1 of its codomain has no preimage. By contrast, the function

$$h : \{0,1,2\} \to \{0,1,4\}, \quad x \mapsto x^2$$

is bijective: 0, 1, and 2 are the unique preimages of 0, 1, and 4, respectively.

To construct the inverse of a function, we must interchange the roles of its domain and codomain, reversing the direction of the elements' correspondences. Since this results in a function if and only if the original function is bijective, an *invertible* function —one that has an inverse— is precisely a bijective function, i.e., one which is both injective and surjective. As functions, *neither addition nor subtraction is invertible*, since none of them is injective: $(1,0)$, $(0,1)$ are two distinct preimages of 1 under addition, and $(1,0)$, $(2,1)$ are two distinct preimages of 1 under subtraction. This, on the one hand, already justifies why the sentence (1) is conceptually incorrect if interpreted literally. On the other hand, it naturally motivates the following four questions concerning the injectivity and surjectivity of an operation.

Question 1. *Is there an operation which is neither injective nor surjective?*

Question 2. *Is there an operation which is injective but not surjective?*

Question 3. *Is there an operation which is surjective but not injective?*

Question 4. *Is there an operation which is both injective and surjective?*

Question 1 is easy to answer: yes, the operation $(x,y) \mapsto 0$ on $\mathbb{R}$. So is Question 3: yes, both addition and subtraction on $\mathbb{R}$ are surjective, since for every $x \in \mathbb{R}$ we have $x \pm 0 = x$, but not injective for the aforementioned reason. How about Questions 2 and 4?

3 Injective operations

Both Questions 2 and 4 concern the existence of an injective operation. This is trivial if we allow operations on singletons, i.e., single-element sets; every such operation is both injective and surjective. We are therefore interested only in the existence of an injective operation on a non-singleton. Let us first assume that such an operation $\oplus : A \times A \to A$ exists, and investigate some properties that $\oplus$ must possess.

Firstly, if A is finite, then the injectivity of $\oplus$ forces $|A|^2 = |A \times A| \leqslant |A|$, which implies that A is a singleton, a contradiction. This establishes the following property.

Proposition 4. *An injective operation on a non-singleton, if it exists, can only be defined on an infinite set.*

For the second property, we need the notion of an *idempotent* under an operation, i.e., an element which is equal to its own square [4, page 19].

Definition 5. An element $a \in A$ is an *idempotent* under $\oplus$ if $a \oplus a = a$.

The second property is that $\oplus$ cannot induce a *global* idempotence, i.e., it cannot allow *every* element of A to be an idempotent. Indeed, if every element of A is an idempotent under $\oplus$, then for every $a, b \in A$ we have that $a \oplus b$ is an idempotent, i.e., $(a \oplus b) \oplus (a \oplus b) = a \oplus b$, which, by the injectivity of $\oplus$, implies $a \oplus b = a$ and $a \oplus b = b$, meaning that $a = b$. This implies that A is a singleton, a contradiction. We have therefore proved the following property.

Proposition 6. *An injective operation on a non-singleton, if it exists, cannot allow every element to be an idempotent.*

Let us next show that $\oplus$ cannot be associative or commutative. If it is, then for every $a \in A$ we have $a \oplus (a \oplus a) = (a \oplus a) \oplus a$ which, by injectivity of $\oplus$, implies $a \oplus a = a$. That is, every element of A is an idempotent under $\oplus$, contradicting our last proposition. Therefore, we have the following.

Proposition 7. *An injective operation on a non-singleton, if it exists, is neither associative nor commutative.*

Furthermore, if $\oplus$ possesses a *left identity* [4, page 25]: an element $e \in A$ such that $e \oplus a = a$ for every $a \in A$, then for every $a \in A$ we have $e \oplus (a \oplus e) = a \oplus e$, and so $e = a$, by injectivity, implying that A is a singleton, a contradiction. A similar argument applies in the case of $\oplus$ possessing a *right identity*.

Proposition 8. *An injective operation on a non-singleton, if it exists, has neither left nor right identity.*

Finally, suppose that $\oplus$ obeys the *Latin square property* [4, 5]: for every $a, b \in A$ there exist $x, y \in A$ such that $a \oplus x = b$ and $y \oplus a = b$. Then, for every $a \in A$ there exist $x, y \in A$ such that $a = a \oplus x = y \oplus a$, which means that $x = y = a$ by injectivity, and so $a \oplus a = a$. That is, every element of A is an idempotent under $\oplus$, a contradiction.

Proposition 9. *An injective operation on a non-singleton, if it exists, cannot obey the Latin square property.*

Summarising our propositions, an injective operation on a non-singleton, if it exists, must be defined on an infinite set, not allow a global idempotence, be neither associative nor commutative, have no identity, and not satisfy the Latin square property. Such an operation, therefore, must be rather pathological! What could be an example?

4 Examples of injective operations on non-singletons

Let us give three examples of an injective operation on a non-singleton, and hence answers to Questions 2 and 4. Our first example —the simplest one— is number-theoretical; its injectivity relies on the uniqueness of prime factorisations, which is guaranteed by the *fundamental theorem of arithmetic* [9, Theorem 3.13].

Theorem 10. *Every integer greater than* 1 *has a prime factorisation —an expression of the integer as a product of one or more primes— which is unique up to reordering of the factors.*

Thus, the equations

$$2^a3^b = 12 = 2^2 3^1 \qquad \text{and} \qquad 2^a3^b = 60 = 2^2 3^1 5^1$$

have the unique positive-integer solution $(a, b) = (2, 1)$ and no positive-integer solution, respectively.

Example 11. Fix two distinct primes p and q. Define the following operation on the set $\mathbb{N}$ of positive integers:

$$\oplus : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad (a, b) \mapsto p^a q^b.$$

Then, any codomain element whose only prime factors are p and q, has a unique preimage under $\oplus$, by the uniqueness of prime factorisations. On the other hand, any codomain element which is divisible by a prime other than p and q, has no preimage under $\oplus$. This shows that $\oplus$ is injective but not surjective. We have therefore provided a positive answer to Question 2.

Our second example uses the concept of a *binary tree*, a special type of *directed graph*. Let us first recall the necessary definitions [1, 7].

Definition 12. A *graph* is an ordered pair $G = (V, E)$ consisting of a finite set V of *vertices* and a set E of *edges*: *unordered* pairs of distinct vertices. A *directed graph* is an ordered pair $G = (V, E)$ consisting of a finite set V of *vertices* and a set E of *arcs*: *ordered* pairs of distinct vertices. By treating every arc of a directed graph as an edge, we obtain a graph, which is the *underlying graph* of the directed graph.

For example, $G_1 = (\{1, 2, 3, 4\}, \{(1, 2), (1, 4), (3, 1), (4, 3)\})$ is the directed graph which can be drawn as the leftmost diagram in Figure 1: each vertex is drawn as a circular node, and each arc (v_1, v_2) as an arrow from v_1 to v_2. In the same figure, $G_2 = (\{1, 2, 3, 4\}, \{\{1, 2\}, \{1, 4\}, \{3, 1\}, \{4, 3\}\})$ is a graph, which is the underlying graph of G_1.

Definition 13. Let $G = (V, E)$ be a directed graph. A *directed subgraph* of G is a directed graph $G' = (V', E')$ such that $V' \subseteq V$ and $E' \subseteq E$. If $V' \subseteq V$, then the *directed subgraph of* G *induced by* V' is $G[V'] = (V', \{(v_1, v_2) \in E : v_1, v_2 \in V'\})$, obtained from G by retaining only all vertices in V' and all arcs whose components are both in V'.

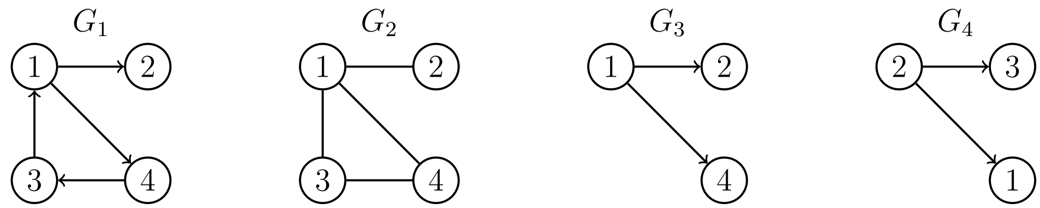

Figure 1: Examples of graphs and directed graphs.

For the directed graph G_1 in Figure 1, we have that $G_1[\{1,2,4\}] = (\{1,2,4\},\{(1,2),(1,4)\}) = G_3$; that is, G_3 is the directed subgraph of G_1 induced by the vertex subset $\{1,2,4\}$.

Definition 14. Two directed graphs $G = (V, E)$ and $G' = (V', H')$ are *isomorphic*, written $G \cong G'$, if there is a bijective function $f : V \to V'$ such that $(v_1, v_2) \in E$ if and only if $(f(v_1), f(v_2)) \in E'$.

Intuitively, two graphs are isomorphic if one of them can be transformed to the other by merely renaming the vertices. For example, the directed graphs G_3 and G_4 in Figure 1 are isomorphic, i.e., $G_3 \cong G_4$, via the bijective function —the vertex-renaming— given by $1 \mapsto 2$, $2 \mapsto 3$, and $4 \mapsto 1$.

Definition 15. In a graph $G = (V, E)$, a *path* is a finite sequence $(v_1, v_2, \ldots, v_n)$ of vertices such that $\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_{n-1}, v_n\} \in E$. The sequence is called a *cycle* if, in addition, $\{v_n, v_1\} \in E$. The graph G is *connected* if there is a path beginning and ending at every pair of its vertices. The graph G is a *tree* if it is connected but has no cycle.

Thus, the graph G_2 in Figure 1 is connected. In this graph, the sequences $(4, 3, 1, 2)$ and $(1, 4, 3)$ are both paths. Since the latter (but not the former) is a cycle, G_2 is not a tree.

Definition 16. In a directed graph $G = (V, E)$, the *in-degree* of a vertex $v_i \in V$ is the number of vertices $v_j \in V$ such that $(v_j, v_i) \in E$. The *out-degree* of the same vertex is the number of vertices $v_j \in V$ such that $(v_i, v_j) \in E$.

In the graph G_1 in Figure 1, the in-degrees of the vertices 1, 2, 3, and 4 are all 1, while their out-degrees are 2, 0, 1, and 1, respectively.

Definition 17. A directed graph is a *directed tree* if its underlying graph is a tree. A directed tree is a *rooted tree* if there is a unique vertex, called the *root*, with in-degree 0, and the in-degree of every other vertex is 1. In a rooted tree, the *level* of a vertex is the length of a path connecting the root and that vertex in the underlying graph, and an *intermediate vertex* is a vertex having a non-zero out-degree. Finally, a rooted tree is a *binary tree* if the out-degree of every intermediate vertex is at most 2.

Thus, the graph G_3 in Figure 1 is a binary tree with root 1, and no intermediate vertices. The levels of the vertices 1, 2, and 4 are 0, 1, and 1, respectively.

Example 18. Let $\mathcal{T}$ be the set of all binary trees with non-empty vertex sets, whose vertices are labelled with consecutive natural numbers starting from 1 by increasing level, and for each level, from left to right[6]. Figure 2 displays some examples of trees in $\mathcal{T}$.

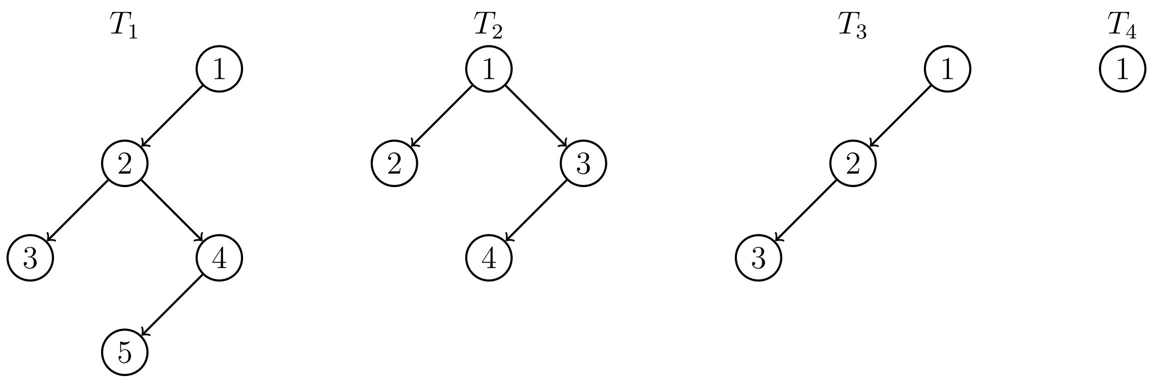

Figure 2: Examples of trees in $\mathcal{T}$.

Let us now define an operation $\oplus$ on $\mathcal{T}$. Given $T_1, T_2 \in \mathcal{T}$, construct $T_1 \oplus T_2$ as follows. First, place the binary trees T_1 and T_2 side by side. Then, add a new vertex which is joined with an arc to the root of T_1, and with another arc to the root of T_2. This gives a new binary tree, whose vertices are finally relabelled according to the above convention. For example, if T_1 and T_2 are as in Figure 2, then $T_1 \oplus T_2$ is the tree in Figure 3. More formally, for every $T_1, T_2 \in \mathcal{T}$, $T_1 \oplus T_2$ is the unique binary tree T in $\mathcal{T}$ having the property that $\{\{1\}, V, V'\}$ is the only partition of the vertex set of T such that $2 \in V$, $3 \in V'$, $T[V] \cong T_1$, and $T[V'] \cong T_2$.

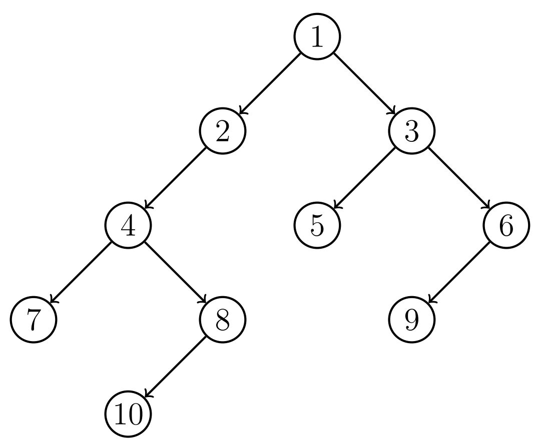

Figure 3: The tree $T_1 \oplus T_2$, where T_1 and T_2 are as in Figure 2.

[6]This is the so-called *shelling order* [11].

Now, let $T = (V, E) \in \mathcal{T}$. If the out-degree of the root v of T is equal to 2, as with T_1 and T_2 in Figure 2, then T has a unique preimage under $\oplus$, which is the ordered pair consisting of the two maximal connected directed subgraphs of $T[V \smallsetminus \{v\}]$. Otherwise, the out-degree of v is less than 2, as with T_3 and T_4 in Figure 2; in this case T has no preimage under $\oplus$. Thus, the operation $\oplus$ is injective but not surjective, thereby providing another answer to Question 2.

Our final example is defined on the set $\mathbb{N}$ of non-negative integers, exploiting the decimal representations of integers.

Example 19. For every $x, y \in \mathbb{N}$, define $x \oplus y$ to be the positive integer constructed by writing the digits of x and of y from left to right in alternation. For example, $123 \oplus 456 = 142536$. If the number of digits k and ℓ of the operands are not equal, then we first add $k - \ell$ zeros in front of the smaller operand. Thus, to compute $123 \oplus 56$, we regard 56 as '056', obtaining 102536. Similarly, to compute $23 \oplus 456$, we regard 23 as '023', obtaining '042536', i.e., the integer 42536.

The definition of $\oplus$ can be extended to the set $\mathbb{N}_0$ of non-negative integers. If exactly one of the operands is 0, we regard this zero as a string of as many zeros as the number of digits of the other operand. That is, to compute $123 \oplus 0$ and $0 \oplus 123$, we regard 0 as '000', obtaining, in the former case, 102030, and, in the latter case, '010203', i.e., the integer 10203. Finally, define $0 \oplus 0$ to be 0.

Written formally, for every $x, y \in \mathbb{N}_0$, define

$$x \oplus y := \begin{cases} \overline{a_n b_m a_{n-1} b_{m-1} a_{n-2} b_{m-2} \cdots a_1 b_1 a_0 b_0}\,, & \text{if } x, y \neq 0 \text{ and } n = m\,; \\ \overline{b_m 0 b_{m-1} 0 b_{m-2} \cdots 0 b_{n+1} a_n b_n a_{n-1} b_{n-1} \cdots a_1 b_1 a_0 b_0}\,, & \text{if } x, y \neq 0 \text{ and } n < m\,; \\ \overline{a_n 0 a_{n-1} 0 a_{n-2} 0 \cdots a_{m+1} 0 a_m b_m a_{m-1} b_{m-1} \cdots a_1 b_1 a_0 b_0}\,, & \text{if } x, y \neq 0 \text{ and } n > m\,; \\ \overline{b_m 0 b_{m-1} 0 b_{m-2} \cdots 0 b_1 0 b_0}\,, & \text{if } x = 0 \text{ and } y \neq 0\,; \\ \overline{a_n 0 a_{n-1} 0 a_{n-2} 0 \cdots a_1 0 a_0 0}\,, & \text{if } x \neq 0 \text{ and } y = 0\,; \\ 0\,, & \text{if } x = y = 0\,, \end{cases}$$

where, in every case in which $x \neq 0$, we write

$$x = \overline{a_n a_{n-1} a_{n-2} \cdots a_1 a_0}\,,$$

where the a_is are the decimal digits of x, and in every case in which $y \neq 0$, we write

$$y = \overline{b_m b_{m-1} b_{m-2} \cdots b_1 b_0}\,,$$

where the b_is are the decimal digits of y.[7]

The well-definedness and the injectivity of $\oplus$ both follow immediately from the uniqueness of decimal representations. To prove its surjectivity, let $z \in \mathbb{N}_0$. We seek to write $z = x \oplus y$ for some $x, y \in \mathbb{N}_0$. If $z = 0$, then $z = 0 \oplus 0$, and we are done.

[7]Thus, the overlined expressions are *not* products.

Now, suppose $z \neq 0$ and write $z = \overline{c_k c_{k-1} c_{k-2} c_{k-3} \cdots c_3 c_2 c_1 c_0}$. Two cases need to be considered.

CASE I: k is odd
In this case, $k = 2\ell + 1$ for some $\ell \in \mathbb{N}_0$, so $z = \overline{c_{2\ell+1} c_{2\ell} c_{2\ell-1} c_{2\ell-2} \cdots c_3 c_2 c_1 c_0}$.
If $c_{2\ell} = c_{2\ell-2} = \cdots = c_2 = c_0 = 0$, then $z = \overline{c_{2\ell+1} c_{2\ell-1} c_{2\ell-5} \cdots c_3 c_1} \oplus 0$.
Otherwise, $c_i \neq 0$ for some $i \in \{0, 2, 4, \ldots, 2\ell\}$. Assume that this i is maximal. Then

$$\begin{aligned} z &= \overline{c_{2\ell+1} 0 c_{2\ell-1} 0 c_{2\ell-3} 0 \cdots c_{i+2} 0 c_{i+1} c_i c_{i-1} c_{i-2} \cdots c_3 c_2 c_1 c_0} \\ &= \overline{c_{2\ell+1} c_{2\ell-1} c_{2\ell-3} \cdots c_3 c_1} \oplus \overline{c_i c_{i-2} \cdots c_2 c_0}\,. \end{aligned}$$

CASE II: k is even
In this case, $k = 2\ell$ for some $\ell \in \mathbb{N}_0$, so $z = \overline{c_{2\ell} c_{2\ell-1} c_{2\ell-2} c_{2\ell-3} \cdots c_3 c_2 c_1 c_0}$.
If $c_{2\ell-1} = c_{2\ell-3} = \cdots = c_3 = c_1 = 0$, then $z = 0 \oplus \overline{c_{2\ell} c_{2\ell-2} c_{2\ell-4} \cdots c_2 c_0}$.
Otherwise, $c_i \neq 0$ for some $i \in \{1, 3, 5, \ldots, 2\ell - 1\}$. Assume that this i is maximal. Then

$$\begin{aligned} z &= \overline{c_{2\ell} 0 c_{2\ell-2} 0 c_{2\ell-4} \cdots 0 c_{i+1} c_i c_{i-1} c_{i-2} \cdots c_3 c_2 c_1 c_0} \\ &= \overline{c_i c_{i-2} \cdots c_2 c_0 \cdots c_3 c_1} \oplus \overline{c_{2\ell} c_{2\ell-2} c_{2\ell-4} \cdots c_2 c_0}\,. \end{aligned}$$

Thus, the operation $\oplus$ on $\mathbb{N}_0$ is both injective and surjective, and thus invertible, thereby providing an answer to Question 4. On the other hand, notice that the same operation $\oplus$ defined on $\mathbb{N}$ is injective but not surjective, since, e.g., every single-digit integer has no preimage; this provides yet another answer to Question 2.

Notice that the operation in the last example can be defined more generally by replacing decimal representations with *base-r representations* [9, section 2.2], for any fixed $r \in \mathbb{N}$ with $r \geqslant 2$.

Acknowledgments

The third author thanks Giovanni Rosalia for a discussion which initiates the writing of this article.

References

[1] V.K. Balakrishnan, *Introductory Discrete Mathematics*, Dover Publications, New York, 1991.

[2] P.J. Cameron, *Introduction to Algebra*, 2^{nd} edition, Oxford University Press, Oxford, 2008.

[3] C.B. Ebby, E.T. Hulbert, and R.M. Broadhead, *A Focus on Addition and Subtraction: Bringing Mathematics Education Research to the Classroom*, Routledge, New York, 2021.

[4] J.B. Fraleigh and N.E. Brand, *A First Course in Abstract Algebra*, 8th edition, Pearson, New Jersey, 2021.

[5] J.A. Gallian, *Contemporary Abstract Algebra*, 10th edition, CRC Press, Boca Raton, 2021.

[6] D. Haylock and A.D. Cockburn, *Understanding Mathematics for Young Children: A Guide for Foundation Stage and Lower Primary Teachers*, SAGE Publications, London, 2008.

[7] L.H. Hsu and C.K. Lin, *Graph Theory and Interconnection Networks*, CRC Press, Boca Raton, 2009.

[8] R. Jorgensen, *Teaching Mathematics in Primary Schools: Principles for Effective Practice*, Routledge, 2020.

[9] T. Koshy, *Elementary Number Theory with Applications*, 2nd edition, Elsevier, 2007.

[10] L. Ma, *Knowing and Teaching Elementary Mathematics: Teachers' Understanding of Fundamental Mathematics in China and the United States*, Routledge, 2010.

[11] P. Rosenstiehl, Scaffold permutations, *Discrete Math.* **75** (1989), 335–342.

[12] C. Wheater, *Basic Math and Pre-Algebra: Tutorial and Practice Problems*, Penguin Group, New York, 2014.