

Algebraic Structure in a Family of Nim-like Arrays

Lowell Abrams *
Department of Mathematics
The George Washington University
Washington, DC 20052 U.S.A.
labrams@gwu.edu

Dena S. Cowen-Morton
Department of Mathematics
Xavier University
Cincinnati, OH 45207-4441 U.S.A.
morton@xavier.edu

September 10, 2009

Abstract

We study aspects of the algebraic structure shared by a certain family of recursively generated arrays related to the operation of Nim-addition. We first observe that each individual array represents a countably infinite, commutative loop (in the sense of quasigroups). We then prove that each loop in the family is monogenic (generated by a single element in a non-associative fashion), and use this to determine all loop homomorphisms between members of the family.

Keywords: quasigroups and loops, monogenic, Nim, Sprague-Grundy, sequential compound

MSC: 20N05, 91A46

1 Introduction

The game of Nim is a two-person combinatorial game in which the players alternate turns removing any number of stones they wish from a single pile of stones; the winner is the player who takes the last stone. The direct sum $G_1 \oplus G_2$ of two combinatorial games G_1, G_2 is the game in which a player, on their turn, has the option of making a move in exactly one of the games G_1 or G_2 which are not yet exhausted (in Nim this simply means having several independent piles of stones). Again, the winner is the last player to make a move. The importance of Nim was established by the Sprague-Grundy Theorem [8, 16] (also developed in [4, chapter 11]), which essentially asserts that Nim is universal among

*Partially supported by The Johns Hopkins University's Acheson J. Duncan Fund for the Advancement of Research in Statistics

finite, impartial two-player combinatorial games in which the winner is the player to move last. Briefly, that is to say that every such game G is, vis-a-vis direct sum, equivalent to a single-pile Nim game; we write $|G|$ for the size of that single pile, and call it the “Grundy-value” of G .

In [17], Stromquist and Ullman define an operation on games called “sequential compound”. Essentially, the sequential compound $G \rightarrow H$ of games G and H is the game in which play proceeds in G until it is exhausted, at which point play switches to H . In this paper we explore combinatorial games whose structure is $(G_1 \oplus G_2) \rightarrow H$, where G_1, G_2 , and H are individual combinatorial games. Previously, little was understood about this type of sequential compound in the case that H is equivalent to a Nim-pile with more than one stone in it (if H is equivalent to a Nim-pile with one stone in it, this is called *misère* play). Our results here cover sequential compounds of this type for piles of any size.

The Sprague-Grundy Theorem implies that direct-sum of Nim-piles yields an operation, called Nim-addition, on $\mathbb{N} \cup \{0\}$, and it is well known that Nim-addition may be represented as a recursively generated array [2]. The purpose of this paper is to give a detailed algebraic description of the members of a family $\mathcal{A}_* = \{\mathcal{A}_s\}_{s \in \mathbb{N} \cup \{0\}}$ of related recursively generated arrays corresponding to a combination of direct sum and sequential compound. The subscript s corresponds to the Grundy-value of the game H ; the array \mathcal{A}_0 is thus the Nim-addition table itself, and the array \mathcal{A}_1 arises from *misère* play [2]. The array \mathcal{A}_2 was first mentioned in [17], where Stromquist and Ullman commented that it “reveals many curiosities but few simple patterns.” The results and observations in this paper were developed by the authors to algebraically explain some of those many curiosities, not just for \mathcal{A}_2 but for all \mathcal{A}_s .

Until recently, there appears to have been no other discussion in the literature of \mathcal{A}_* or the “sequential compound” operation introduced in [17] which gave rise to these arrays, other than a brief mention in a list of problems compiled by Richard Guy [9, Problem 41]. Recently, however, Rice described each of the arrays \mathcal{A}_s as endowing $\mathbb{N} \cup \{0\}$ with the algebraic structure of a quasigroup [13].

In contrast to the situation for \mathcal{A}_* , there has been a fair amount of discussion regarding an array arising in the study of Wythoff’s game [2, 3, 5, 10, 11, 14]. In the recent paper [14], Rice defines a family of arrays generalizing Wythoff’s game in essentially the same way as \mathcal{A}_* generalizes Nim.

The structure of this paper is as follows: In Section 2 we construct the arrays \mathcal{A}_s , and explain how they provide game-winning strategies. The section closes with an algebraic perspective which shows that the arrays \mathcal{A}_s may in fact be viewed as each providing the structure of a loop, which is a quasigroup with identity [12, 15].

In Section 3 we collect some basic results on recurring patterns in the arrays. These are important mainly for their uses in later sections.

In Section 4 we prove the Monogenicity Theorem (Theorem 4.1), which asserts that the loop \mathcal{A}_s is generated by a single element if and only if the seed s satisfies $s \geq 2$. Moreover, for seed $s = 2$ every element $n > s$ is a generator, and for seed $s > 2$ every element $n \neq s$ is a generator. Drawing on the classical work of Evans in [6] we then prove an additional result showing that none of the loops \mathcal{A}_s are finitely-represented. This implies that the results in Evans' sequel [7] regarding loop homomorphisms do not apply in our context.

In Section 5 we prove the Loop Homomorphism Theorem (Theorem 5.1), which gives a complete description of all homomorphisms between the arrays \mathcal{A}_s for most values of s . In particular, the only loop homomorphism $f : \mathcal{A}_s \rightarrow \mathcal{A}_t$ for $s \neq t$ and $s \geq 2$ or $t \geq 2$ is the trivial map $\mathcal{A}_s \rightarrow \{t\}$. For $s = t \geq 2$, a loop homomorphism f is either the trivial map $\mathcal{A}_s \rightarrow \{s\}$ or the identity map.

In Section 6 we first provide structural results explicating the structures of \mathcal{A}_0 and \mathcal{A}_1 in terms of a quotient map $\mathcal{A}_1 \rightarrow \mathcal{A}_0$. We then use this information to classify the homomorphisms from \mathcal{A}_s to \mathcal{A}_t where $s, t \in \{0, 1\}$. For these cases, in sharp contrast to the findings of the Loop Homomorphism Theorem in Section 5, there are infinitely many choices for each homomorphism.

Due the universality of Nim, the Monogenicity Theorem shows that every combinatorial game is equivalent to a game that can be obtained from [almost] any pair of combinatorial games, using various combinations of direct sum and sequential compound, where one of the two games plays the role of the game H above. In other words, it is a kind of decomposition theorem for games. The Loop Homomorphism Theorems of Sections 5 and 6 then tell us that there are infinitely many distinct ways to go about this, even for the same choice of H .

A graphical approach to the arrays \mathcal{A}_s , as well as proofs of various periodicity properties enjoyed by these arrays, may be found in our paper [1]. Further algebraic properties, beyond those that appear in this article, will be discussed elsewhere. We conclude in Section 7 with a description of one of these properties.

We note that our algebraic analysis of the arrays \mathcal{A}_s differs from that in [13]. Our approach naturally gives rise to an identity element, and no result analogous to the Monogenicity Theorem appears in [13]. Although an analogue of Section 5 appears in [13], our proof differs in that it relies essentially on Section 4.

Acknowledgements. The first author had several helpful conversations with Robbie Robinson and Daniel Ullman. Michael Cowen and Daniel Otero offered helpful suggestions during the writing stage. Charles Weibel contributed to Theorems 6.4 and 6.6. The comments of an anonymous referee led to important improvements in the paper. The first author thanks the Department of Applied Mathematics and Statistics at The Johns Hopkins University for their gracious hospitality and support during the development of this article.

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 0 & 3 & 2 & 5 & 4 & 7 & 6 \\ 2 & 3 & 0 & 1 & 6 & 7 & 4 & 5 \\ 3 & 2 & 1 & 0 & 7 & 6 & 5 & 4 \\ 4 & 5 & 6 & 7 & 0 & 1 & 2 & 3 \\ 5 & 4 & 7 & 6 & 1 & 0 & 3 & 2 \\ 6 & 7 & 4 & 5 & 2 & 3 & 0 & 1 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \end{bmatrix}$$

Figure 1: $\mathcal{A}_0(7, 7)$

2 Mex and the Arrays \mathcal{A}_s

We begin by constructing a family of infinite arrays using the mex operation:

Definition 2.1 For a set X of non-negative integers we define $\mathbf{mex} X$ to be the smallest non-negative integer not contained in X . Here, \mathbf{mex} stands for **m**inimal **e**xcluded value.

Definition 2.2 For any 2-dimensional array \mathcal{M} indexed by $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, let $\mathbf{a}_{i,j}$ denote the entry in row i , column j , where $i, j \geq 0$. The **principal (i, j) subarray $\mathcal{M}(i, j)$** is the subarray of \mathcal{M} consisting of entries $a_{p,q}$ with indices $(p, q) \in \{0, \dots, i\} \times \{0, \dots, j\}$. For $j \geq 0$ define **Left (i, j)** to be the set of all entries in row i to the left of the entry $a_{i,j}$, and for $i \geq 0$ define **Up (i, j)** to be the set of entries in column j above $a_{i,j}$. (Note that $\text{Left}(i, 0) = \text{Up}(0, j) = \emptyset$.)

Definition 2.3 The infinite array \mathcal{A}_s , for $s \in \mathbb{N}_0$, is constructed recursively: The seed $a_{0,0}$ is set to s and for $(i, j) \neq (0, 0)$,

$$a_{i,j} := \mathbf{mex} \left(\text{Left}(i, j) \cup \text{Up}(i, j) \right).$$

See, for example, Figures 1 and 2.

The array \mathcal{A}_0 is well known as the Nim addition table, and has been extensively studied in the setting of combinatorial game theory. In particular, the i, j -entry of \mathcal{A}_0 is equal to the Grundy-value $|G_1 \oplus G_2|$ where G_1 is a game with $|G_1| = i$ and G_2 is a game with $|G_2| = j$; see [2] for more details. Consideration of what is known as “misère play” gives rise to the array \mathcal{A}_1 . (The reader can easily verify that this change of seed from 0 to 1 has a minimal effect; other than the top left 2×2 block, the pattern of this array is exactly the same as that of \mathcal{A}_0 .) Using the sequential compound construction of Stromquist and Ullman [17] gives rise to the full family of arrays \mathcal{A}_s . Indeed, the i, j -entry of \mathcal{A}_s is $|(G_1 \oplus G_2) \rightarrow *s|$ where

2	0	1	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	2	4	3	6	5	8	7	10	9	12	11	14	13	16
1	2	0	5	6	3	4	9	10	7	8	13	14	11	12	17
3	4	5	0	1	2	7	6	9	8	11	10	13	12	15	14
4	3	6	1	0	7	2	5	11	12	13	8	9	10	16	18
5	6	3	2	7	0	1	4	12	11	14	9	8	15	10	13
6	5	4	7	2	1	0	3	13	14	12	15	10	8	9	11
7	8	9	6	5	4	3	0	1	2	15	14	16	17	11	10
8	7	10	9	11	12	13	1	0	3	2	4	5	6	17	19
9	10	7	8	12	11	14	2	3	0	1	5	4	16	6	20
10	9	8	11	13	14	12	15	2	1	0	3	6	4	5	7
11	12	13	10	8	9	15	14	4	5	3	0	1	2	7	6
12	11	14	13	9	8	10	16	5	4	6	1	0	3	2	21
13	14	11	12	10	15	8	17	6	16	4	2	3	0	1	5
14	13	12	15	16	10	9	11	17	6	5	7	2	1	0	3
15	16	17	14	18	13	11	10	19	20	7	6	21	5	3	0

Figure 2: $\mathcal{A}_2(15, 15)$

G_1, G_2 have Grundy-values i and j , respectively, and $*s$ denotes the s -stone, single-pile Nim game.

Having the arrays \mathcal{A}_s in hand has a direct usefulness when playing a game $(G_1 \oplus G_2) \rightarrow *s$. A Grundy-value of 0 indicates that the “previous” player to move (*i.e.*, the player who is not making the next move) has a winning strategy, and any nonzero Grundy-value indicates that the next player to move has a winning strategy. If $|G_1| = i$ and $|G_2| = j$, then for each $a \in \text{Up}(i, j)$ there is a move in G_1 (depending on the specifics of G_1) that results in a new game G'_1 such that $|(G'_1 \oplus G_2) \rightarrow *s| = a$. Similarly, for $a \in \text{Left}(i, j)$ there is a move in G_2 that results in a new game G'_2 such that $|(G_1 \oplus G'_2) \rightarrow *s| = a$.

We present some of the practical implications: If $s = 0$ and $|G_1| < |G_2|$ then a move in $G = (G_1 \oplus G_2) \rightarrow *s$ which leaves G_1 alone and changes G_2 to a game with Grundy-value $|G_1|$ is a winning move. If $s > 0$ and $1 < |G_1| < |G_2|$ then the same is true, but when $|G_1| = 1$ the winning move is to change G_2 to a game with Grundy-value 0, and when $|G_1| = 0$ the winning move is to change G_2 to a game with Grundy-value 1.

It may appear that only the location of the 0 values in \mathcal{A}_s is of concern for game-playing, but this is not the case. To see that the full information of the array \mathcal{A}_s is useful, consider games of the form $((G_1 \oplus G_2) \rightarrow *s) \oplus G_3$. In this case, a winning move in $(G_1 \oplus G_2) \rightarrow *s$ could be a losing move overall (for instance, if G_3 is a single Nim-pile). On the other hand, a move in G_1 to a game G'_1 such that $|(G'_1 \oplus G_2) \rightarrow *s| = |G_3|$, for example, would be a winning move, and thus knowledge of the locations of entries in \mathcal{A}_s equal to $|G_3|$ is quite

useful.

Several properties of \mathcal{A}_s follow as immediate consequences of the recursive construction:

Proposition 2.4 *For each s , the array \mathcal{A}_s is symmetric, and each nonnegative integer appears exactly once in each row (and, by symmetry, each column).*

While this holds for \mathcal{A}_0 and \mathcal{A}_2 equally, it is evident from Figure 2 above that \mathcal{A}_2 is not at all regular, in direct contrast to \mathcal{A}_0 . Although the entries in \mathcal{A}_0 can be calculated directly (*i.e.*, non-recursively) using bitwise XOR [2], we have not found any non-recursive way to calculate entries of \mathcal{A}_s for any $s \geq 2$ (and suspect that such an algorithm does not exist). A different recursive algorithm for constructing \mathcal{A}_s (an analogue of “Algorithm WSG” in [3]) is described in [1].

We now describe our algebraic perspective on \mathcal{A}_s . For a fixed s , view \mathcal{A}_s as providing the “multiplication table” for an operation $*: \mathbb{N}_0 \times \mathbb{N}_0 \rightarrow \mathbb{N}_0$, where row 0 and column 0 correspond to multiplication by the seed s . Thus, s is the $*$ -identity, and $i * j := a_{i',j'}$ where i' and j' are such that $a_{i',0} = i$ and $a_{0,j'} = j$. In practice, to perform the $*$ operation and find $i * j$, one simply looks at the intersection of the row with initial entry i and the column with initial entry j . For example, for $j > s$ we have $a_{0,j} = s * j$, and for $j > s \geq 1$ we have $a_{1,j} = 0 * j$. For all s , if $i, j > s$ then $a_{i,j} = i * j$. Thus, in \mathcal{A}_2 we have $1 * 4 = 6$ and $3 * 6 = 7$ (see Figure 2).

Definition 2.5 ([12, 15]) *A quasigroup $(Q, *)$ is a set Q with binary operation $*: Q \times Q \rightarrow Q$ such that for every $i, j \in Q$ there exist unique $p, q \in Q$ such that $i * p = j$ and $q * i = j$. A loop $(L, *)$ is a quasigroup with identity element $e \in L$ such that for every $i \in L$, $e * i = i = i * e$.*

Theorem 2.6 *For each s , the array \mathcal{A}_s defines a countably infinite, commutative loop structure on \mathbb{N}_0 .*

Proof. By Proposition 2.4, $*$ is a commutative operation. Moreover, that proposition also shows that for each $j \in \mathbb{N}_0$, the left- and right-multiplication maps $L_j, R_j: \mathbb{N}_0 \rightarrow \mathbb{N}_0$ given by $L_j(i) = j * i$ and $R_j(i) = i * j$ for all $i \in \mathbb{N}_0$ are bijections, *i.e.*, $*$ has a cancellation property. Thus, the algebraic structure $(\mathbb{N}_0, *)$ is a quasigroup. Since $(\mathbb{N}_0, *)$ has a $*$ -identity (namely, s) it is moreover a loop. \square

It is important to note that although $(\mathbb{N}_0, *)$ is a group when $s = 0$ (in that case, $*$ is bitwise-XOR), for $s \geq 1$ the operation $*$ is not even associative. For example, in seed $s = 1$ we have $(2 * 2) * 4 = 0 * 4 = 5$, but $2 * (2 * 4) = 2 * 6 = 4$.

In the following sections we will refer to \mathcal{A}_s both as an array and as the corresponding loop.

3 Pattern Properties for \mathcal{A}_s

We collect in this section various results describing the pattern of entries in \mathcal{A}_s ; these will be used heavily in other sections. Properties 3.1-3.5 describe multiplication by s , 0, 1, 2, and 3 (for most seeds). Properties 3.6-3.8 give the locations of the elements 0, 1 and 3 in the array (for various seeds). Properties 3.9 and 3.10 present two relations involving iterated products of a single element. Although we observed and proved these properties independently, proofs of some of the observations in this section have been recorded in [13]. All proofs are by strong induction. For Properties 3.6-3.8 note that the placement of an entry equal to i depends only on the placement of entries less than or equal to i .

The first property shows that s is the $*$ -identity in \mathcal{A}_s for all s .

Property 3.1 *For all $n \in \mathbb{N}_0$,*

$$s * n = n.$$

The next property gives the result of $*$ -multiplication by 0 except when $s = 0$; the latter case is covered by Property 3.1.

Property 3.2 *If $s > 0$ and $n \leq s$ then*

$$0 * n = \begin{cases} 0 & \text{if } n = s \\ n + 1 & \text{otherwise} \end{cases}$$

If $s > 0$ and $n > s$ then

$$0 * n = \begin{cases} n - 1 & \text{if } n - s \equiv 0 \pmod{2} \\ n + 1 & \text{if } n - s \equiv 1 \pmod{2} \end{cases}$$

The next property gives the result of $*$ -multiplication by 1 (except when $s = 1$, which is covered by Property 3.1).

Property 3.3 *If $s = 0$ then*

$$1 * n = \begin{cases} n + 1 & \text{if } n \equiv 0 \pmod{2} \\ n - 1 & \text{if } n \equiv 1 \pmod{2} \end{cases}$$

If $s \geq 2$ and $n < s$ then

$$1 * n = \begin{cases} n + 2 & \text{if } n \equiv 0, 2 \pmod{3} \\ n - 1 & \text{if } n \equiv 1 \pmod{3} \end{cases}$$

If $s \geq 2$ and $n > s$ then

$$1 * n = \begin{cases} n - 1 & \text{if } s \equiv 0 \pmod{3} \text{ and } n = s + 1 \\ n - 2 & \text{if } s \equiv 1 \pmod{3} \text{ and } n = s + 1 \\ n + 1 & \text{if } s \equiv 0, 1 \pmod{3} \text{ and } n > s + 1 \text{ and } n - s \equiv 0 \pmod{2} \\ n - 1 & \text{if } s \equiv 0, 1 \pmod{3} \text{ and } n > s + 1 \text{ and } n - s \equiv 1 \pmod{2} \\ n - 2 & \text{if } s \equiv 2 \pmod{3} \text{ and } n - s \equiv 0, 3 \pmod{4} \\ n + 2 & \text{if } s \equiv 2 \pmod{3} \text{ and } n - s \equiv 1, 2 \pmod{4} \end{cases}$$

Note that the given cases when $s \equiv 2 \pmod{3}$ include the possibility that $n = s + 1$.

The next property gives all but the first few results of $*$ -multiplication by 2 for seeds $s \geq 5$.

Property 3.4 If $4 \leq n < s$ then

$$2 * n = \begin{cases} n + 3 & \text{if } n \equiv 0, 1, 5 \pmod{9} \\ n - 1 & \text{if } n \equiv 2, 3, 6, 8 \pmod{9} \\ n + 2 & \text{if } n \equiv 4, 7 \pmod{9} \end{cases}$$

If $n > s \geq 5$ then

$$2 * n = \begin{cases} n - 2 & \text{if } s \equiv 0, 4 \pmod{9} \text{ and } n - s \equiv 0, 3 \pmod{4} \\ n + 2 & \text{if } s \equiv 0, 4 \pmod{9} \text{ and } n - s \equiv 1, 2 \pmod{4} \\ n + 2 & \text{if } s \equiv 1, 6 \pmod{9} \text{ and } n > s + 1 \text{ and } n - s \equiv 0 \pmod{2} \\ n - 2 & \text{if } s \equiv 1, 6 \pmod{9} \text{ and } n > s + 1 \text{ and } n - s \equiv 1 \pmod{2} \\ n + 2 & \text{if } s \equiv 2 \pmod{9} \text{ and } n - s \equiv 0, 3 \pmod{4} \\ n - 2 & \text{if } s \equiv 2 \pmod{9} \text{ and } n - s \equiv 1, 2 \pmod{4} \\ n - 2 & \text{if } s \equiv 3, 7 \pmod{9} \text{ and } n > s + 1 \text{ and } n - s \equiv 0, 1 \pmod{4} \\ n + 2 & \text{if } s \equiv 3, 7 \pmod{9} \text{ and } n > s + 1 \text{ and } n - s \equiv 2, 3 \pmod{4} \\ n + 1 & \text{if } s \equiv 5, 8 \pmod{9} \text{ and } n > s + 1 \text{ and } n - s \equiv 0 \pmod{2} \\ n - 1 & \text{if } s \equiv 5, 8 \pmod{9} \text{ and } n > s + 1 \text{ and } n - s \equiv 1 \pmod{2} \\ n - 1 & \text{if } s \equiv 1, 5, 7 \pmod{9} \text{ and } n = s + 1 \\ n - 2 & \text{if } s \equiv 3, 6, 8 \pmod{9} \text{ and } n = s + 1 \end{cases}$$

The next property gives all but the first few results of $*$ -multiplication by 3 for seed $s = 2$.

Property 3.5 For $s = 2$ and $n \geq 6$ we have

$$3 * n = \begin{cases} n + 1 & \text{if } n \equiv 0 \pmod{2} \\ n - 1 & \text{if } n \equiv 1 \pmod{2} \end{cases}$$

The following property describes the placement of entries equal to 0 for all seeds s .

Property 3.6 For all seeds s and all n ,

$$n * n = \begin{cases} 1 & \text{if } n = 0 \text{ and } s > 0 \\ s & \text{if } n = s \\ 0 & \text{otherwise} \end{cases}$$

The next property describe the placements of the entries equal to 1 for seeds $s = 0, 1, 2$.

Property 3.7 For $s = 0, 1$ and $m, n \geq 2$ we have $m * n = 1$ if and only if $\{m, n\} = \{2k, 2k + 1\}$ for some $k \geq 1$. For $s = 2$ and $m, n \geq 3$ we have $m * n = 1$ if and only if $\{m, n\} = \{2k + 1, 2k + 2\}$ for some $k \geq 1$.

The next property describes the placement of the entries equal to 3 for the case seed $s = 2$. We will use this in the proof of the Monogenicity Theorem (Theorem 4.1).

Property 3.8 For $s = 2$ and $m, n \geq 6$ we have $m * n = 3$ if and only if $\{m, n\} = \{2k, 2k + 1\}$ for some $k \geq 3$.

The final properties in this section will also be useful in the proof of Theorem 4.1.

Property 3.9 For $s = 2$ and $n \neq 0, s$ we have $n * (n * (n * n)) = 1$.

Property 3.10 In \mathcal{A}_s where $s \geq 2$, we have $\underbrace{0 * (\dots * (0 * 0))}_n = n - 1$ for all $1 \leq n \leq s + 1$.

4 Monogenicity

Let $\langle x, \diamond \rangle$ denote the free unital groupoid [12] with operation \diamond on a single generator x . Thus, $\langle x, \diamond \rangle$ contains a \diamond -identity e_\diamond and all possible parenthesizations of \diamond -products of x , each of which is a distinct element. A loop \mathcal{L} with identity element $e_\mathcal{L}$ is said to be **monogenic** if there is an element $n \in \mathcal{L}$ such that the operation-respecting map (groupoid homomorphism) $\phi_n: \langle x, \diamond \rangle \rightarrow \mathcal{L}$ determined by $\phi_n(e_\diamond) = e_\mathcal{L}$ and $\phi_n(x) := n$ is surjective. In this case, n is said to be a **generator** of \mathcal{L} . Note that our notion of monogenicity is

slightly stronger than the one used in [7], which would correspond to using a free *loop* on a single generator in place of $\langle x, \diamond \rangle$.

Given an element $\ell \in \mathcal{L}$, we refer to any element $q \in \langle x, \diamond \rangle$ such that $\phi_n(q) = \ell$ as a **shape** of ℓ . Since the map ϕ_n need not be injective, an element of \mathcal{L} can have more than one shape. For simplicity, we write x^k to denote $(L_x)^k(e_\diamond)$ (recall that L_x denotes the left-multiplication map; see Theorem 2.6), and n^k to denote $\phi_n(x^k)$. For example, if $\gamma \in \langle x, \diamond \rangle$ is the shape $(x \diamond x) \diamond (x \diamond x)$ then $\phi_n(\gamma) = (n * n) * (n * n) = (n^2)^2$. Observe that in this notation Property 3.6 refers to n^2 , Property 3.9 refers to n^4 , and Property 3.10 refers to 0^n .

Theorem 4.1 (Monogenicity Theorem) *The loop \mathcal{A}_s is monogenic if and only if the seed s satisfies $s \geq 2$. For seed $s = 2$, every element $n > s$ is a generator, and for $s > 2$, every element $n \neq s$ is a generator.*

Proof. This proof refers repeatedly to the properties of Section 3; in particular we will use Property 3.6 without further comment. There are, in addition, a number of “special case” computations which the reader can easily carry out by hand.

Case 1: $s = 0$.

We have $n * n = 0$ for all $n \in \mathbb{N}$. Since 0 is the $*$ -identity, each element n generates only $\{0, n\}$.

Case 2: $s = 1$.

For $n > 1$, we have $n * n = 0$, so n such that $n > 1$ generates either $\{n, 0, n-1, 1\}$ (if n is odd) or $\{n, 0, n+1, 1\}$ (if n is even). It is easy to check that for $n = 0$ just $\{0, 1\}$ is generated. Of course, $n = 1$ does not generate, since it is the $*$ -identity.

Case 3: $s = 2$.

First note that none of the elements 0, 1, 2 generate; in fact, $\{0, 1, 2\}$ is a group under $*$. We proceed by showing that the element 3 generates, and then that for each $n > 3$, the element n generates 3.

Since $3^2 = 0, 3^3 = 4, 3^4 = 1, 3^5 = 5$, and $3^6 = 2$, we see that 3 generates all elements $2k$ and $2k+1$ for $k \leq 2$. Proceeding by induction on k , if 3 generates $2k$ and $2k+1$, then since $3^2 * (2k+1) = 0 * (2k+1) = 2k+2$ and $3 * (2k+2) = 2k+3$, we see that 3 generates $2(k+1)$ and $2(k+1)+1$. This shows that 3 is a generator when $s = 2$.

We now consider $n > 3$ when $s = 2$. We have $4^3 = 3, 5 * (5^2 * 5^2) = 3$, and $6^2 * 6^5 = 3$, so $n = 4, 5, 6$ all generate. Letting $\phi_n: \langle x, \diamond \rangle \rightarrow \mathcal{A}_2$ denote “evaluation at n ,” we now note that for each $n \geq 7$ either $\phi_n(x^3 \diamond x^5) = 3$ or $\phi_n(x \diamond [x^3 \diamond x^4]) = 3$. To show this, we argue mod 4 using various properties from Section 3:

1. If $n = 4k+1$ for some $k \geq 2$, then $n * [n^3 * n^4] = n * [(n * 0) * 1] = (4k+1) * [(4k+2) * 1] = (4k+1) * (4k) = 3$.

2. If $n = 4k + 2$ for some $k \geq 2$, then $n^3 * n^5 = (n * 0) * (n * 1) = (4k + 1) * (4k) = 3$.
3. If $n = 4k + 3$ for some $k \geq 1$, then $n^3 * n^5 = (n * 0) * (n * 1) = (4k + 4) * (4k + 5) = 3$.
4. If $n = 4k + 4$ for some $k \geq 1$, then $n * [n^3 * n^4] = n * [(n * 0) * 1] = (4k + 4) * [(4k + 3) * 1] = (4k + 4) * (4k + 5) = 3$

It follows that when $s = 2$ every $n > 2$ generates the element 3, hence the entire loop \mathcal{A}_2 .

Case 4: $s > 2$.

In these cases we will show that 0 is a generator. From this it will follow that every n with $n \neq s$ is a generator of \mathcal{A}_s , since for $n \neq 0, s$ we have $n^2 = 0$. Of course, s is the identity element, so it does not generate.

By Property 3.10 we have $0^k = k - 1$ for all seeds $s > 2$ and for $k = 1, 2, 3, \dots, s + 1$. Thus 0 generates all of the elements $0, \dots, s$.

For seeds $s \equiv 0, 1 \pmod{3}$ we have $0^2 * 0^s = 1 * (s - 1) = s + 1$; for seeds $s \equiv 2 \pmod{9}$ we have $0^3 * 0^{s-1} = 2 * (s - 2) = s + 1$; and for seeds $s \equiv 5, 8 \pmod{9}$ we have $0^3 * 0^s = 2 * (s - 1) = s + 1$. Thus 0 generates $s + 1$.

For all seeds s , $0 * (s + 1) = s + 2$. Thus 0 generates all of the elements $0, \dots, s + 2$.

Sub-Case 4a: $s > 2$ and $s \equiv 0, 1 \pmod{3}$.

We have $0^2 * (s + j) = 1 * (s + j) = s + j + 1$ for j even with $j \geq 2$, and $0 * (s + j) = s + j + 1$ for j odd with $j \geq 1$. Thus, a simple proof by induction shows that 0 generates \mathcal{A}_s for seeds $s \equiv 0, 1 \pmod{3}$.

Sub-Case 4b: $s > 2$ and $s \equiv 2 \pmod{3}$.

We have $0^2 * (s + 1) = 1 * (s + 1) = s + 3$ and $0^2 * (s + 2) = 1 * (s + 2) = s + 4$. Thus, we can generate through $s + 4$.

For seeds $s \equiv 5, 8 \pmod{9}$ we have $0^3 * (s + 4) = 2 * (s + 4) = s + 5$ and for seeds $s \equiv 2 \pmod{9}$ we have $0^3 * (s + 3) = 2 * (s + 3) = s + 5$. Thus 0 generates $0, \dots, s + 5$, for $s \equiv 2 \pmod{3}$.

Proceeding by induction on a variable j we assume that 0 generates $s + 1, s + 4j + 2, s + 4j + 3, s + 4j + 4$, and $s + 4j + 5$ for $0 \leq j \leq J$; we have proven this for $j = 0$ above. Since for all $k \geq 1$ we have (noting that $1 = 0^2$ and $2 = 0^3$)

$$\begin{aligned}
0 * (s + 4k + 1) &= s + 4k + 2 \\
1 * (s + 4k + 1) &= s + 4k + 3 \\
0 * (s + 4k + 3) &= s + 4k + 4 \\
2 * (s + 4k + 4) &= s + 4k + 5 \quad \text{for } s \equiv 5, 8 \pmod{9} \\
2 * (s + 4k + 3) &= s + 4k + 5 \quad \text{for } s \equiv 2 \pmod{9},
\end{aligned}$$

the induction is completed by taking $k = J + 1$ in these identities. \square

A loop is said to be **finitely-related** if it can be described in terms of generators and relations using only finitely many relations.

Proposition 4.2 *The loop \mathcal{A}_s is not finitely-related for any seed s .*

Proof. We first show that for each seed s , each element n in \mathcal{A}_s satisfies a relation $\phi_n(w) = s$ for some $w \in \langle x, \diamond \rangle$; from this it follows that \mathcal{A}_s does not contain a free subloop. In \mathcal{A}_0 we may take $w = x^2$. In \mathcal{A}_1 we may take $w = (x^2)^2$. In \mathcal{A}_s for $s \geq 2$ we take $w = (x^2)^{s+1}$ for $n \neq 0$, and $w = x^{s+1}$ for $n = 0$. That each of these choices of w has the required property follows from Propositions 3.2, 3.6, and 3.10.

Now \mathcal{A}_s is infinite and, by Theorem 4.1, finitely generated. Since an infinite finitely-generated loop which is finitely-related contains a free subloop [6, §3.3], it must be that \mathcal{A}_s is not finitely related. \square

5 The Loop Homomorphism Theorem

Theorem 5.1 (Loop Homomorphism Theorem) *The only loop homomorphism $f : \mathcal{A}_s \rightarrow \mathcal{A}_t$ for $s \neq t$ and either $s \geq 2$ or $t \geq 2$ (or both) is the trivial map $\mathcal{A}_s \rightarrow \{t\}$. For $s = t \geq 2$ a homomorphism f is either the trivial map $\mathcal{A}_s \rightarrow \{s\}$ or the identity map.*

Proof. Let $s, t \in \mathbb{N}_0$ and let $f : \mathcal{A}_s \rightarrow \mathcal{A}_t$ be a loop homomorphism. Recall that s is the identity element of \mathcal{A}_s for all s . We have $f(s) * f(s) = f(s * s) = f(s) = f(s) * t$ so $f(s) = t$ for all f , by the cancellation property (see Theorem 2.6). We let $\phi_m : \langle x; \diamond \rangle \rightarrow \mathcal{A}_s$ and $\psi_m : \langle x; \diamond \rangle \rightarrow \mathcal{A}_t$ denote evaluation homomorphisms as in Section 4.

As before, we use various properties from Section 3 without explicit mention. The proof is broken into cases, according to the values of s and t .

Case 1: $s, t \geq 2$ and $f(a) = 0$ or $f(a) = t$ for some $a \neq 0, s$.

Suppose first $f(a) = t$ for some $a \neq 0, s$. Then

$$f(0) = f(a * a) = f(a) * f(a) = t * t = t$$

so $f(0) = t$ also. But then for all $i \neq 0, s$ we have

$$t = f(0) = f(i * i) = f(i) * f(i),$$

which can only occur if $f(i) = t$. Thus f is the trivial map.

Suppose now that $f(a) = 0$ for some $a \neq 0, s$. Then

$$f(0) = f(a * a) = f(a) * f(a) = 0 * 0 = 1.$$

Let b, b' be mutual inverses in \mathcal{A}_s , where $b, b' \neq 0, a, s$. Then $1 = f(0) = f(b*b) = f(b)*f(b)$ means that $f(b) = 0$, and likewise $f(b') = 0$. But $t = f(s) = f(b*b') = f(b)*f(b') = 0*0 = 1$, which is a contradiction to $t \geq 2$.

Case 2: $s, t \geq 2$ and $f(a) \neq 0, t$ for any $a \neq 0, s$.
Suppose $a \neq 0, s$. We then have

$$f(0) = f(a*a) = f(a)*f(a) = 0,$$

and Property 3.10 now gives $n = 0^{n+1} = f(0^{n+1}) = f(n)$ for all $1 \leq n \leq s$. Thus f is the identity map for all $0 \leq n \leq s$, and in particular, $f(s) = s$. Since we know that $f(s) = t$, this gives us that Case 2 may only occur if $s = t$, *i.e.*, different seeds give non-isomorphic loops.

Note that for $s = t > 2$, the fact that 0 is a generator (by Theorem 4.1), together with $f(0) = 0$ as shown above, forces f to be the identity map $\mathcal{A}_s \rightarrow \mathcal{A}_s$.

Now we consider $s = t = 2$. Let $f: \mathcal{A}_2 \rightarrow \mathcal{A}_2$ be a loop endomorphism. By the hypothesis of Case 2 we have $f(3) \neq 0, 2$. It is also true that $f(3) \neq 1$, since otherwise we have

$$1 = f(3) = f(0*4) = f(0)*f(4) = 0*f(4),$$

which forces $f(4) = 0$, contradicting the hypothesis of Case 2. Thus $f(3) \geq 3$. We first show that $f(3) \leq 6$, then verify that $f(3) \neq 4, 5, 6$.

Let $\omega \in \langle x, \diamond \rangle$ denote the shape $\omega = \left[x^2 \diamond \left((x^2)^2 \diamond x \right) \right]$ and let $\alpha, \beta \in \langle x, \diamond \rangle$ denote the shapes

$$\alpha = (x^2)^2 \diamond \omega \quad \text{and} \quad \beta = ((x^2)^2 \diamond x) \diamond (x \diamond \omega).$$

Using various Pattern Properties we can calculate that $\phi_3(\alpha) = 4 = \phi_3(\beta)$. This gives

$$\phi_{f(3)}(\alpha) = f \circ \phi_3(\alpha) = f \circ \phi_3(\beta) = \phi_{f(3)}(\beta).$$

We will now show that for $s = t = 2$ and $f(3) = n > 6$ we in fact have $\phi_n(\alpha) \neq \phi_n(\beta)$, and thus $f(3) = n \leq 6$. (The fact that this works only for $n > 6$ is due to the hypothesis of Property 3.5.)

First, we calculate $\phi_n(\alpha)$ for $n > 6$:

$$\begin{aligned}
\phi_n(\alpha) = 1 * [0 * (1 * n)] &= \begin{cases} 1 * [0 * (n - 2)] & \text{if } n - 2 \equiv 0, 3 \pmod{4} \\ 1 * [0 * (n + 2)] & \text{if } n - 2 \equiv 1, 2 \pmod{4} \end{cases} \\
&= \begin{cases} 1 * [n - 3] & \text{if } n - 2 \equiv 0 \pmod{4} \\ 1 * [n - 1] & \text{if } n - 2 \equiv 3 \pmod{4} \\ 1 * [n + 3] & \text{if } n - 2 \equiv 1 \pmod{4} \\ 1 * [n + 1] & \text{if } n - 2 \equiv 2 \pmod{4} \end{cases} \\
&= \begin{cases} n - 1 & \text{if } n - 2 \equiv 0 \pmod{2} \\ n + 1 & \text{if } n - 2 \equiv 1 \pmod{2} \end{cases}
\end{aligned}$$

Now we calculate $\phi_n(\beta)$ for $n > 6$:

$$\begin{aligned}
\phi_n(\beta) = (1 * n) * (n * [0 * (1 * n)]) &= \begin{cases} (n - 2) * (n * [0 * (n - 2)]) & \text{if } n - 2 \equiv 0, 3 \pmod{4} \\ (n + 2) * (n * [0 * (n + 2)]) & \text{if } n - 2 \equiv 1, 2 \pmod{4} \end{cases} \\
&= \begin{cases} (n - 2) * (n * [n - 3]) & \text{if } n - 2 \equiv 0 \pmod{4} \\ (n - 2) * (n * [n - 1]) & \text{if } n - 2 \equiv 3 \pmod{4} \\ (n + 2) * (n * [n + 3]) & \text{if } n - 2 \equiv 1 \pmod{4} \\ (n + 2) * (n * [n + 1]) & \text{if } n - 2 \equiv 2 \pmod{4} \end{cases}
\end{aligned}$$

By Properties 3.5 and 3.8 we have $\phi_n(\beta) = (n + 2) * 3 = n + 3$ for $n \equiv 0 \pmod{4}$ and $\phi_n(\beta) = (n - 2) * 3 = n - 3$ for $n \equiv 1 \pmod{4}$. Thus $\phi_n(\alpha) \neq \phi_n(\beta)$ for $n \equiv 0, 1 \pmod{4}$, where $n > 6$.

To show that $\phi_n(\alpha) \neq \phi_n(\beta)$ for other values of n , note that we must show that

$$(n - 2) * (n * [n - 3]) \neq n - 1 \text{ when } n \equiv 2 \pmod{4},$$

and that

$$(n + 2) * (n * [n + 3]) \neq n + 1 \text{ when } n \equiv 3 \pmod{4}.$$

But by Property 3.5, for any n with $n \equiv 2 \pmod{4}$, $n > 6$ the unique solution y to $(n - 2) * y = n - 1$ is 3, and for any n with $n \equiv 3 \pmod{4}$, $n > 6$ the unique solution y to $(n + 2) * y = n + 1$ is also 3. By Property 3.8, it is not the case that $n * [n - 3] = 3$, nor that $n * [n + 3] = 3$, and thus $\phi_n(\alpha) \neq \phi_n(\beta)$ for $n \equiv 2, 3 \pmod{4}$, where $n > 6$.

From this we see that $f(3) = n$ must satisfy $f(3) \leq 6$.

Now let $\omega \in \langle x, \diamond \rangle$ denote the shape $\omega = x^2 \diamond (x \diamond [(x^2)^2 \diamond (x^2 \diamond x)])$ and consider the shapes $\gamma, \delta \in \langle x, \diamond \rangle$ given by

$$\gamma = (x^2 \diamond x) \diamond ((x^2)^2 \diamond \omega) \quad \text{and} \quad \delta = ((x^2)^2 \diamond [x^2 \diamond x]) \diamond \omega.$$

It is straightforward to verify that $\phi_3(\gamma) = 13 = \phi_3(\delta)$ but $\phi_n(\gamma) \neq \phi_n(\delta)$ for $n = 4, 5, 6$. Thus, $f(3) \neq 4, 5, 6$. We have shown that $f(3) = 3$; since 3 is a generator of \mathcal{A}_2 by Theorem 4.1, it follows that f is the identity map.

Case 3: $s = 0, 1$ and $t \geq 2$

First, let $s = 0$. For any $n \in \mathcal{A}_0$ we have

$$[f(n)]^2 = f(n^2) = f(0) = t.$$

Since $t \geq 2$, this tells us that $f(n) = t$ for all n .

Now let $s = 1$. For any $n \in \mathcal{A}_1$ we have

$$([f(n)]^2)^2 = f([n^2]^2) = f(1) = t.$$

Since $t \geq 2$, this tells us that $[f(n)]^2 = t$ and thus $f(n) = t$ for all n .

Case 4: $s \geq 2$ and $t = 0, 1$

First, take $s > 2$. For $m > s$, say, we can see that

$$f(1) = f((m^2)^2) = ([f(m)]^2)^2 = t.$$

Since 1 is a generator of \mathcal{A}_s , we see that f is trivial.

We now take $s = 2$. For a shape $\gamma \in \langle x; \diamond \rangle$ let $|\gamma|$ denote the number of x 's appearing in γ .

Sub-Case 4a: $s = 2$ and $t = 0$

Recall that $\psi_n: \langle x; \diamond \rangle \rightarrow \mathcal{A}_t$ is the evaluation map sending x to n . Because \mathcal{A}_0 is associative, for any shape γ and any m , we have

$$f \circ \phi_m(\gamma) = \psi_{f(m)}(x^{|\gamma|}) = \begin{cases} f(m) & \text{if } |\gamma| \equiv 1 \pmod{2} \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

Now let $\omega \in \langle x; \diamond \rangle$ denote the shape $\omega = \left(x \diamond \left[x^3 \diamond (x^2)^2 \right] \right)$ and let $\gamma, \delta \in \langle x; \diamond \rangle$ denote the shapes

$$\gamma = (x^2)^2 \diamond \omega \quad \text{and} \quad \delta = x \diamond (x^2 \diamond \omega).$$

Note that $\phi_3(\gamma) = 9 = \phi_3(\delta)$, but $|\gamma| = 12 \neq 11 = |\delta|$. By Equation (1) we have

$$0 = f \circ \phi_3(\gamma) = f \circ \phi_3(\delta) = \psi_{f(3)}(\delta) = f(3).$$

Since 3 generates \mathcal{A}_2 , we see that f is trivial.

Sub-Case 4b: $s = 2$ and $t = 1$

From the relation $f(1) = f(0) * f(0)$ we see that $f(1)$ is either 0 or 1. The observation

$$1 = f(2) = f(0 * 1) = f(0) * f(1)$$

therefore implies that $f(0) = f(1) \in \{0, 1\}$. But the relation $f(1) = f(0) * f(0)$ precludes $f(0) = f(1) = 0$, and thus $f(0) = f(1) = f(2) = 1$. Since, for any $n > 2$, we have

$$1 = f(0) = f(n) * f(n)$$

it follows that $\text{im } f \subseteq \{0, 1\}$. Since $\{0, 1\}$ is an associative subloop of \mathcal{A}_1 , we see that for any shape γ and any m we have

$$f \circ \phi_m(\gamma) = \psi_{f(m)}(x^{|\gamma|}) = \begin{cases} f(m) & \text{if } |\gamma| \equiv 1 \pmod{2} \\ 1 & \text{otherwise} \end{cases}$$

We may now complete the proof, *mutatis mutandis*, using the shapes γ and δ as in Subcase 4a.

□

6 Homomorphisms and Structure of \mathcal{A}_0 and \mathcal{A}_1

In this section, we let $*_0$ and $*_1$ denote the operations in \mathcal{A}_0 and \mathcal{A}_1 , respectively. Recall, as remarked at the end of Section 2, that \mathcal{A}_0 is associative while \mathcal{A}_1 is not.

Proposition 6.1

1. If $m > 1$ and $n > 1$ then $m *_1 n = m *_0 n$.
2. If $l, m, n > 1$ and also $l *_1 m > 1$ and $m *_1 n > 1$, then $(l *_1 m) *_1 n = l *_1 (m *_1 n)$.
3. For any m, n we have $(0 *_1 m) *_1 n = 0 *_1 (m *_1 n)$.
4. For any $m, n \in \mathcal{A}_0$ we have $m *_0 (m *_0 n) = n$. For any $m, n \in \mathcal{A}_1$ with $m, n, m *_1 n > 1$ we have $m *_1 (m *_1 n) = n$.

Proof. Statement 1 follows from the observation that the arrays \mathcal{A}_0 and \mathcal{A}_1 differ only in their respective top left 2×2 subarrays. Statement 2 then follows from the first, since \mathcal{A}_0 is associative.

To verify statement 3, note first that for $m, n > 1$ it is true that $0 *_1 m > 1$, so by statement 1 we have $(0 *_1 m) *_1 n = (0 *_1 m) *_0 n = (1 *_0 m) *_0 n = 1 *_0 (m *_0 n) = 0 *_1 (m *_1 n)$. (Note that the last equality holds even when $m *_1 n = 0, 1$.) By commutativity and the pattern properties the remaining cases ($m = 0, 1$ or $n = 0, 1$) follow easily.

The case of \mathcal{A}_0 in statement 4 follows from associativity and Property 3.6. By statement 1, the case of \mathcal{A}_1 then follows from \mathcal{A}_0 . □

Let $S = \{2^i | i = 0, 1, 2, \dots\}$ and $S' = \{2^i | i = 1, 2, 3, \dots\}$. Observe that each element $2^i \in S$ generates a subgroup H_i in \mathcal{A}_0 isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Since the operation in \mathcal{A}_0 is bitwise XOR, \mathcal{A}_0 is the weak product of these H_i for $i = 0, 1, 2, \dots$

Now note that each element in S' generates a subgroup $G_i = \{2^i, 0, 2^i+1, 1\}$ in \mathcal{A}_1 isomorphic to $\mathbb{Z}/4\mathbb{Z}$. All G_i contain the subgroup $\{0, 1\}$, so \mathcal{A}_1 is not the weak product of the G_i . Nevertheless, we have:

Proposition 6.2

1. *The elements in S' generate \mathcal{A}_1 , and for each even element $m > 0$ of \mathcal{A}_1 there is a unique subset $S_m \subset S'$ such that m can be expressed as the product of the distinct elements of S_m .*
2. *If $m \in G_i$, $n \in G_j$, $m, n > 1$ and $m *_1 n \in \{0, 1\}$ then $i = j$.*

Proof. The second statement follows from the stronger assertion that if $m, n > 1$ satisfy $m *_1 n \in \{0, 1\}$ then $m, n \in \{2k, 2k + 1\}$ for some k . This, in turn, follows immediately from Properties 3.6 and 3.7.

Since the product in \mathcal{A}_1 of various distinct powers of 2 is always even, the argument above shows that the elements 0 and 1 cannot arise as a product of distinct powers of 2. Because $*_0$ is bitwise XOR, and for each $k > 0$ the element $2k$ can be expressed in \mathcal{A}_0 as a product of the elements of a unique set of distinct elements of S' , the same holds in \mathcal{A}_1 , by Proposition 6.1. Since in \mathcal{A}_1 it holds that $0 = 2^2$, $1 = 2^4$ and for each $k > 0$ we have $2k + 1 = 0 *_1 2k$, the first statement holds as well. \square

We can now formalize the strong relationship between \mathcal{A}_0 and \mathcal{A}_1 .

Theorem 6.3 *Let Q_1 denote the loop quotient of \mathcal{A}_1 by the relation $0 \equiv 1$, let Q_2 denote the loop quotient of \mathcal{A}_1 by the family of relations $\{2k \equiv 2k + 1 | k = 1, 2, \dots\}$, and let Q_3 denote the loop quotient of \mathcal{A}_1 by all relations enforcing associativity. Then each of these three quotients is isomorphic to \mathcal{A}_0 under an isomorphism σ sending the image of G_i to H_{i-1} for each i . Moreover, modulo these isomorphisms the respective corresponding projection maps π_1, π_2 , and π_3 are equal.*

We let Q denote the quotient described by Theorem 6.3 and π the corresponding projection map.

Proof. We first show that Q_1, Q_2 , and Q_3 are the same quotient. If $0 \equiv 1$ then for all $k > 1$, $2k = 1 *_1 2k \equiv 0 *_1 2k = 2k + 1$; thus $2k$ and $2k + 1$ are identified. Conversely, if $2k \equiv 2k + 1$ for $k > 1$ then $0 = 2k *_1 2k \equiv 2k *_1 (2k + 1) = 1$, so $0 \equiv 1$. Thus Q_1 and Q_2 are the same.

Suppose now that $0 \equiv 1$. If any of l, m , or n is equal to 1 then

$$(l *_1 m) *_1 n \equiv l *_1 (m *_1 n). \quad (2)$$

surely holds, and the same will therefore be true if any is equal to 0, since $0 \equiv 1$. Suppose then that $l, m, n > 1$. If $l *_1 m = 0, 1$ then $l = m$ or $l = 0 *_1 m$, which in either case gives $l \equiv m$. Thus, if $l *_1 m = 0, 1$ and $m *_1 n = 0, 1$ then we have $l \equiv m \equiv n$, in which case (2) holds trivially. If $l *_1 m = 0, 1$ but $m *_1 n \neq 0, 1$ then we invoke Proposition 6.1 to obtain

$$(l *_1 m) *_1 n = 0 *_1 n \equiv n = m *_0 (m *_0 n) = m *_1 (m *_1 n) \equiv l *_1 (m *_1 n)$$

as desired. The remaining case not covered by Proposition 6.1 follows by commutativity, and we see that if $0 \equiv 1$ then associativity holds.

Conversely, if associativity holds then for any $m > 1$ we have, by Proposition 6.1,

$$1 = 0 *_1 0 = (m *_1 m) *_1 0 \equiv m *_1 (m *_1 0) = m *_0 (m *_0 0) = 0.$$

We conclude that Q_1 and Q_3 are the same.

We are now justified in speaking about the single quotient Q . Q is an associative loop and hence a group; by Proposition 6.2 it is generated by $[S'] = \{[2^i] | i = 1, 2, 3, \dots\}$, where $[m]$ denotes the class of m . Since $[2^i] * [2^j] = [2^i *_1 2^j] = [2^i *_0 2^j]$, we see that the operation in Q matches that of \mathcal{A}_0 ; Q is thus a weak product of copies of $\mathbb{Z}/2\mathbb{Z}$ generated by $[S']$. It follows that the function $\sigma: Q \rightarrow \mathcal{A}_0$ defined by $\sigma([2^i]) = 2^{i-1}$ for all i extends to an isomorphism of Q to \mathcal{A}_0 . Of course the image of G_i in Q is its image in Q_2 , *i.e.*, it is $\{[0], [2^i]\}$, and $\sigma(\{[0], [2^i]\}) = \{0, 2^{i-1}\} = H_{i-1}$.

The statement regarding the projection maps follows readily from the arguments above. \square

We now account, in this theorem and the next, for the cases not included in Theorem 5.1.

Theorem 6.4

1. $Hom(\mathcal{A}_0, \mathcal{A}_0) = \prod_0^\infty \mathcal{A}_0$
2. $Hom(\mathcal{A}_0, \mathcal{A}_1) = \prod_0^\infty \mathbb{Z}/2\mathbb{Z}$
3. $Hom(\mathcal{A}_1, \mathcal{A}_0) = \prod_0^\infty \mathcal{A}_0$

Proof. Since \mathcal{A}_0 is the weak product of H_i for $i = 0, 1, 2, \dots$, each homomorphism $\mathcal{A}_0 \rightarrow \mathcal{A}_0$ is determined, uniquely and without restriction, by a choice of value in \mathcal{A}_0 for each generator 2^i . Statement 1 now follows.

Similarly, a homomorphism $f: \mathcal{A}_0 \rightarrow \mathcal{A}_1$ is determined by its values on S . However, for each i , $(f(2^i))^2 = f(2^i * 2^i) = f(0) = 1$ forces $f(2^i) \in \{0, 1\}$ by Property 3.6, and thus statement 2 holds.

Given any homomorphism $g: \mathcal{A}_0 \rightarrow \mathcal{A}_0$, the composition $g \circ \sigma \circ \pi$ is a homomorphism $\mathcal{A}_1 \rightarrow \mathcal{A}_0$. We now show that every homomorphism $f: \mathcal{A}_1 \rightarrow \mathcal{A}_0$ arises in this way. Using any $n > 1$ we can see that $f(0) = f(n * n) = f(n) * f(n) = 0$. By Property 3.2 we then have, for any $n > 0$, $f(2n+1) = f(2n * 0) = f(2n) * f(0) = f(2n)$. It follows that f factors through Q as $g \circ \sigma \circ \pi$ for some homomorphism $g: \mathcal{A}_0 \rightarrow \mathcal{A}_0$, and statement 3 holds as a corollary of statement 1. \square

To prove the homomorphism structure from $\mathcal{A}_1 \rightarrow \mathcal{A}_1$ we need a preliminary lemma:

Lemma 6.5 *For any homomorphism $f: \mathcal{A}_1 \rightarrow \mathcal{A}_1$*

1. $f(0) = 0$ or $f(0) = 1$.
2. Either $f(2k) = f(2k+1) = 0$, $f(2k) = f(2k+1) = 1$, or $\{f(2k), f(2k+1)\} = \{2j, 2j+1\}$ for some $j > 0$.
3. If $f(0) = 0$ and $m > 1$, then $f(m) > 1$.
4. If $f(0) = 0$ then f is injective.
5. If $f(0) = 0$ and $\{f(m), f(n)\} = \{2j, 2j+1\}$ for some j then $\{m, n\} = \{2i, 2i+1\}$ for some i .

Proof. Any homomorphism $f: \mathcal{A}_1 \rightarrow \mathcal{A}_1$ must satisfy $f(0) = 0, 1$ since these are the only values that will satisfy $f(0) * f(0) = f(0^2) = f(1) = 1$, proving statement 1. Moreover, statement 2 holds since for any $k > 0$ we have $f(2k) * f(2k+1) = f(1) = 1$ and thus for $k > 0$ either $f(2k) = f(2k+1) = 0$, $f(2k) = f(2k+1) = 1$, or $\{f(2k), f(2k+1)\} = \{2j, 2j+1\}$ for some $j > 0$.

Statement 3 follows from the fact that if $f(0) = 0$, then for any $m > 1$ we have $f(m) * f(m) = f(m^2) = f(0) = 0$, so $f(m) > 1$ as well.

To prove statement 4, we note first that if $n > m+1 > 2$ then $f(m), f(n), f(m * n) > 1$ by statement 3, so by Proposition 6.1 we have

$$f(n) = f[m * (m * n)] = f(m) * [f(m) * f(n)].$$

If $f(m) = f(n)$ then this gives $f(m) = f(m) * 0$, which is a contradiction.

We now consider m, n differing by 1. By statements 2 and 3, for any $k > 0$ we have $\{f(2k), f(2k+1)\} = \{2j, 2j+1\}$ for some j . So in particular $f(2k) \neq f(2k+1)$ for any $k > 0$. Now suppose $f(2k+1) = f(2k+2)$ for some $k > 0$. Then $f((2k+1) * (2k+2)) =$

$f(2k+1) * f(2k+2) = 0$, since $2k+1, 2k+2 > 1$ imply that $f(2k+1) = f(2k+2) > 1$ by statement 3. Then, since $(2k+1) * (2k+2) > 1$ for every $k > 0$, by Proposition 6.1

$$f(2k+1) = f(2k+2) = f(2k+1) * f\left((2k+1) * (2k+2)\right) = f(2k+1) * 0,$$

which is a contradiction, and the injectivity of f is verified.

The last assertion now follows as well. Suppose $\{f(m), f(n)\} = \{2j, 2j+1\}$ for some j . If m is even then $\{f(m), f(m+1)\} = \{2j, 2j+1\} = \{f(m), f(n)\}$, so $f(n) = f(m+1)$, which forces $n = m+1$ by injectivity. Similarly, if m is odd then $n = m-1$. \square

Theorem 6.6 $Hom(\mathcal{A}_1, \mathcal{A}_1) = \prod_1^\infty \mathbb{Z}/2\mathbb{Z} \cup (Inj(\mathcal{A}_0, \mathcal{A}_0) \times \{0, 1\}^{\mathbb{N}_0})$

Proof. Let f be a homomorphism $\mathcal{A}_1 \rightarrow \mathcal{A}_1$. Suppose first that $f(0) = 1$. Then $f(m) = 0, 1$ for all $m > 1$ since these are the only values that will satisfy $f(m) * f(m) = f(m^2) = f(0) = 1$. This in turn implies that $f(2k) = f(2k+1)$ for all $k > 0$, by Lemma 6.5, and thus f factors as $g \circ \pi$ for some homomorphism $g: Q \rightarrow \mathbb{Z}/2\mathbb{Z}$. Since every such g gives rise in this way to an $f: \mathcal{A}_1 \rightarrow \mathcal{A}_1$ with $f(0) = 1$, the set of such f is $\prod_1^\infty \mathbb{Z}/2\mathbb{Z}$.

Suppose now that $f(0) = 0$. It follows from Lemma 6.5 that f is injective and if $\pi \circ f(m) = \pi \circ f(n)$ then either $f(m) = 0 * f(n) = f(0 * n)$ or $f(m) = f(n)$. In either case, $\pi(m) = \pi(n)$. Thus the homomorphism $\pi \circ f: \mathcal{A}_1 \rightarrow Q$ factors as $g \circ \pi$ for some injective homomorphism $g: Q \rightarrow Q$.

By Theorem 6.3 each homomorphism $f: \mathcal{A}_1 \rightarrow \mathcal{A}_1$ satisfying $f(0) = 0$ gives rise in this way to an injective homomorphism $\phi: \mathcal{A}_0 \rightarrow \mathcal{A}_0$. We now show how each possible $f: \mathcal{A}_1 \rightarrow \mathcal{A}_1$ is determined by a pair (ϕ, ϵ) where $\phi: \mathcal{A}_0 \rightarrow \mathcal{A}_0$ is any injective homomorphism and $\epsilon: \mathbb{N}_0 \rightarrow \{0, 1\}$ is any map, completing the proof of Theorem 6.6. Given such a pair (ϕ, ϵ) , define a function $f': S \cup \{0\} \rightarrow \mathcal{A}_1$ by $f'(0) := 0$, $f'(1) := 1$, and $f'(2^i) := 2 \cdot \phi(2^{i-1}) + \epsilon(i)$ for $i = 1, 2, 3, \dots$. Note that for every $2^i \in S'$ we have $f'(2^i) > 1$ by the injectivity of ϕ . We extend f' to a homomorphism $f: \mathcal{A}_1 \rightarrow \mathcal{A}_1$ (see Proposition 6.2); it remains to show that f is well-defined and injective.

By Proposition 6.2 each nonzero even element $2k$ of \mathcal{A}_1 can be expressed as a product of the elements of a unique subset $S_{2k} \subset S'$. By Proposition 6.1 and properties 3.6 and 3.7, every possible parenthisization of these elements gives the same product, so there is no ambiguity in this expression. We now show that f' is injective and that if $f'(2^i) = 2k$ for some i, k then there is no j for which $f'(2^j) = 2k+1$. By properties 3.6 and 3.7 together with Proposition 6.1(2), this suffices to show that there is no ambiguity in defining $f(2k)$ to be the product of the elements of $f'(S_{2k})$. Suppose first that $f'(2^i) = f'(2^j)$. We then have $\epsilon(i) = f'(2^i) \bmod 2 = f'(2^j) \bmod 2 = \epsilon(j)$ and $2^i = 2^j$ follows from the injectivity of ϕ . Suppose now that $f'(2^i) = 2k$ for some i, k . If $f'(2^j) = 2k+1$ for some j then $\epsilon(j) = 1$ and by the injectivity of ϕ the equality $f'(2^j) = f'(2^i) + 1$ would give $2^i = 2^j$, a contradiction.

To express an odd element $2k + 1 > 1$ of \mathcal{A}_1 as a product, some multiplicand must be 0 or odd. Since each odd element greater than 1 is of the form $0 *_1 m$ for some even element m , by Proposition 6.1(3) we see that $f(2k + 1)$ is unambiguously defined as $0 *_1 f(2k) = f(0) *_1 f(2k) = f(0 *_1 2k) = f(2k + 1)$. This completes the proof of well-definedness.

To see that f is injective, suppose that $f(m) = f(n)$ for some m, n . Since $\pi \circ f(m) = \pi \circ f(n)$, we have $\pi(m) = \pi(n)$ by the argument above, which means that $m \in \{n, 0 *_1 n\}$. Because $f(0 *_1 n) = 0 *_1 f(n) \neq f(n)$, it must be that $m = n$. \square

7 Another algebraic property

There is much more to study regarding the algebraic structure of the arrays \mathcal{A}_s . For instance, as mentioned in the introduction, we have found the following:

*For each of the seeds $s = 0, 1, 2, 3, 5, 7$ and each pair i, j satisfying $i > s, j > s$, and $i * j > s$, we have $i * (i * j) = j$.*

Indeed, we have proven this for $s = 0$ and $s = 1$ in Proposition 6.1. Note that this algebraic property amounts to a connection between the row index, the column index, and the value of an entry.

This property seems to not be shared by \mathcal{A}_s for any other seeds s .

References

- [1] L. Abrams and D. S. Cowen-Morton, Periodicity and Other Structure in a Colorful Family of Nim-like Arrays, *preprint*.
- [2] E. R. Berlekamp, J. H. Conway, and R. K. Guy, *Winning Ways For Your Mathematical Plays* volume 1, second edition. A. K. Peters, Natick, Massachusetts, 2001.
- [3] U. Blass and A. S. Fraenkel, The Sprague-Grundy function for Wythoff's game, *Theoret. Comp. Science* **75** (1990) 311-333.
- [4] J. H. Conway, *On Numbers and Games*, second edition. A. K. Peters, Wellesley, Massachusetts, 2001.
- [5] A. Dress, A. Flammenkamp, and N. Pink, Additive periodicity of the Sprague-Grundy function of certain Nim games, *Adv. Appl. Math.* **22** (1999), 249-270.
- [6] T. Evans, On multiplicative systems defined by generators and relations I., *Proc. Cambridge Phil. Soc.* **47** (1951), 637-649.

- [7] T. Evans, On multiplicative systems defined by generators and relations II., *Proc. Cambridge Phil. Soc.* **49** (1953), 579-589.
- [8] P. M. Grundy, Mathematics and Games, *Eureka*, **2** (1939), 6-8.
- [9] R. Guy, Unsolved problems in combinatorial games, in *Games of No Chance*, MSRI Publications **29** Cambridge University Press, Cambridge, 1996, 475-491.
- [10] H. A. Landman, A simple FSM-based proof of the additive periodicity of the Sprague-Grundy function of Wythoff's game. In *More Games of No Chance* (Berkeley, CA, 2000), *Math. Sci. Res. Inst. Publ.* **42**, Cambridge Univ. Press, Cambridge (2002) 383-386.
- [11] G. Nivasch, The Sprague-Grundy function for Wythoff's game: On the location of the g -values. Unpublished M.Sc. Thesis, Weizmann Institute of Science, 2004.
- [12] H. O. Pflugfelder, *Quasigroups and loops: introduction*, *Sigma Series in Pure Mathematics* **7**. Heldermann Verlag, Berlin, (1990).
- [13] T. A. Rice, Greedy quasigroups. *Quasigroups and Related Systems* **16 no. 2** (2008) 103-118.
- [14] T. A. Rice, Wythoff quasigroups. *J. Comb. Math. and Comb. Computing*, to appear.
- [15] J. D. H. Smith and A. B. Romanowska, *Post-modern algebra* Pure and Applied Mathematics, A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, (1999).
- [16] R. P. Sprague, Über mathematische Kampfspiele. *Tôhoku Math. J.* **41** (1935-6), 438-444.
- [17] W. Stromquist and D. Ullman, Sequential compounds of combinatorial games, *Theoret. Computer Science* **119** (1993) 311-321.