Commutative subloop-free loops

Martin Beaudry*, Louis Marchand

Abstract. We describe, in a constructive way, a family of commutative loops of odd order, $n \geq 7$, which have no nontrivial subloops and whose multiplication group is isomorphic to the alternating group $\mathcal{A}_n$.

Keywords: loops, multiplication group, alternating group

Classification: 20N05, 20D06

1. Introduction

We say that a finite loop is *subloop-free* whenever it does not have proper subloops, that is, other than itself and the trivial one-element loop. For example, a reduced subsquare-free latin square (also called N_∞ latin square) is the Cayley table of a subloop-free loop. Subsquare-free latin squares are proved to exist for every n not of the form $2^i 3^j$, with $i, j \geq 1$ [13], and are conjectured to exist for every $n \geq 5$. It is also fairly easy to build a subloop-free loop of any order $n \geq 5$ by an ad hoc method, such as specifying the top half of a Cayley table (a bottom half always exists [11]) where the entries equal to the identity are located in such a way that the table cannot be completed in any way that creates the table of a subloop.

While it is well-known that the cyclic groups of prime order are the only finite associative subloop-free loops, it turns out that finite, nonassociative subloop-free loops are numerous and diverse. We substantiate this statement by proving that, for every odd $n \geq 7$, there exist subloop-free loops which simultaneously satisfy the conditions of being commutative and having a multiplication group isomorphic to the alternating group $\mathcal{A}_n$.

Theorem 1.1. *For every odd $n \geq 7$, there exists a commutative subloop-free loop of order n whose multiplication group is the alternating group $\mathcal{A}_n$.*

We leave aside the loops of even order. Indeed, it is a well-known fact, that in a symmetric $n \times n$ latin square the number of occurrences of a given object on the diagonal has the same parity as n; applying this to the identity element implies that every commutative loop of even order has a subgroup isomorphic to $\mathbb{Z}_2$.

We refer the reader to [3], [6], [16] for detailed background on loops. In this article, all loops are finite. Let G be a loop of order n; its operation is denoted

*Corresponding author.

by an asterisk, e.g. $a * b = c$. To each loop element a we associate its *right and left translations*, R_a and L_a respectively, defined by $R_a(b) = b * a$ and $L_a(b) = a * b$. Both mappings are permutations of G. The translations generate $\mathcal{M}(G) = \langle \{ L_a, R_a \mid a \in G \} \rangle$, the *multiplication group* of G. Note that in a commutative loop, we have $L_a = R_a$ for every a; we then speak of the *translation of* a and use the notation L_a.

Our descriptions and proofs use only basic notions and facts on groups and permutations; they can be found in fundamental texts such as [12], [18] and we assume that they are familiar to the reader.

We denote by $G = \{0, 1, \ldots, n-1\}$ the underlying set of a loop G of order n. To make our descriptions simpler, we write them as if G were a subset of $\mathbb{N}$ and use relations and operations usually encountered in these contexts, such as "$\leq$" and "$+$". We denote by $\mathcal{S}_n$ the symmetric group over G and by $\mathcal{A}_n$ the *alternating group*, which is the set of all even permutations of G. In this article we identify an even permutation by verifying that its cyclic representation contains an even number of cycles of even length.

We regard the multiplication group $\mathcal{M}(G)$ as a subset of $\mathcal{S}_n$; we therefore write statements like "$\mathcal{M}(G) = \mathcal{S}_n$" instead of "$\mathcal{M}(G)$ is isomorphic to $\mathcal{S}_n$".

For a given loop, most of our work is done on its Cayley table, where rows and columns are labelled with the loop's elements, and where entry $[a, b]$ contains the value $a * b$. It is well known that a finite groupoid is a loop iff its Cayley table is a reduced latin square; it is commutative iff the table is symmetric.

The notion of multiplication group of a loop was introduced by Albert [1]. The properties of this group have been the object of extensive study, in particular the question of which groups can be the multiplicative group of a nonassociative loop. The multiplication group of almost every quasigroup of order n is $\mathcal{S}_n$ [4], [10], and it is conjectured that the same holds for loops [5]. Among those multiplication groups other than $\mathcal{S}_n$, the alternating group $\mathcal{A}_n$ can be found for almost every order [8]; out result is thus an alternate proof of this statement for the loops of odd order $n \geq 7$. Conversely, it was proved that certain groups cannot be the multiplication group of a loop, for example the linear groups $\mathrm{PSL}(2, q)$ [17].

2. Proof of the theorem

We prove the theorem by building a family of appropriate loops for $n = 37$ and each $n \geq 43$. The smaller values of n are dealt with in the Appendix, where we give an example of a loop for every odd order $n \leq 41$ not covered by our proof.

The rest of this section is structured as follows. First, we build a $n \times n$ symmetric partially defined latin square, which we call the *template*, and we show that it can be completed to yield the Cayley table of a commutative subloop-free loop whose multiplication group has $\mathcal{A}_n$ as a subgroup, provided that an additional constraint is respected. Next, we show how to fill the template in order to ensure that $\mathcal{M}(G) = \mathcal{A}_n$.

From now on, let $n = 2p + 1$. We denote by $[i, j]$ the cell located at the intersection of row i and column j. We call an entry the content of this cell and

	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
0	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1	20	**3**	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	**21**
2	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	**1**	**3**
3	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	**1**	**2**	**0**
4	23	24	25	26	27	28	29	30	31	32	33	34	35	36	**1**	**0**	**3**	**2**
5	24	25	26	27	28	29	30	31	32	33	34	35	36	**2**	**0**	**3**	**4**	**1**
6	25	26	27	28	29	30	31	32	33	34	35	36	**3**	**1**	**5**	**2**	**0**	**4**
7	26	27	28	29	30	31	32	33	34	35	36	**1**	**2**	**0**	**3**	**4**	**5**	6
8	27	28	29	30	31	32	33	34	35	36	?	?	?	?	**4**	**5**	6	7
9	28	29	30	31	32	33	34	35	36	?	?	?	?	?	**2**	6	7	8
10	29	30	31	32	33	34	35	36	?	?	?	?	?	?	6	7	8	9
11	30	31	32	33	34	35	36	?	?	?	?	?	?	6	7	8	9	10
12	31	32	33	34	35	36	?	?	?	?	?	?	6	7	8	9	10	11
13	32	33	34	35	36	?	?	?	?	?	?	6	7	8	9	10	11	12
14	33	34	35	36	**1**	?	?	?	?	?	6	7	8	9	10	11	12	13
15	34	35	36	**2**	**0**	?	?	?	?	6	7	8	9	10	11	12	13	14
16	35	36	**3**	**1**	**5**	?	?	?	6	7	8	9	10	11	12	13	14	15
17	36	**1**	**2**	**0**	**3**	**4**	**5**	6	7	8	9	10	11	12	13	14	15	16
18	**1**	**2**	**0**	**3**	**4**	**5**	6	7	8	9	10	11	12	13	14	15	16	17
19	**3**	**0**	**5**	**4**	**2**	6	7	8	9	10	11	12	13	14	15	16	17	18
20	.	**5**	**4**	**21**	6	7	8	9	10	11	12	13	14	15	16	17	18	19
21	.	.	**1**	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
22	.	.	.	7	8	9	10	11	12	13	14	15	16	17	18	19	20	**5**
23	.	.	.	.	9	10	11	12	13	14	15	16	17	18	19	20	21	22

FIGURE 1. Template for $n = 37$

denote it also by $[i,j]$. Since the table we build is symmetric, we only specify $[i,j]$ for $i \leq j$.

The template is obtained from a totally unspecified $n \times n$ table in several steps. The first step consists in filling most of the cells as if we were building the Cayley table of the cyclic group $\mathbb{Z}_n$.

- For all i,j such that $i+j \leq n-1$ or $i+j \geq n+6$, let $[i,j] = i+j \ (mod\ n)$.

Next, three of these entries are modified, as follows:

- $[1,2] = 0$; $[1,p+2] = 3$; $[p+4,n-1] = 5$.

Still undefined is the width-6 region consisting of those cells $[i,j]$ for which $i \leq j$ and $n \leq i+j \leq n+5$; we call it the *corridor*. Now we partially define the content of the corridor by specifying, on and above the diagonal, a total of 57 entries taken from the set $\{0,1,2,3,4,5\}$, with two exceptions:

- $[1,n-1] = p+3$; $[p+2,p+4] = p+3$.

For the 55 other entries, we refer the reader to Figure 1, where the top right part of the template is displayed for $n = 37$. (With the sole exception of position $[1,2]$, the top left part is identical to its counterpart in the Cayley table of $\mathbb{Z}_n$.) In this figure, the entries below the main diagonal are not represented. The entries in those cells where the template is identical to the table of $\mathbb{Z}_n$, i.e. those where $[i,j] \equiv i+j \ (mod\ n)$, are printed in standard font. Unspecified entries are identified with a question mark "?"; they form a set of contiguous cells, the *undefined zone*. The remaining 59 entries are printed in boldface; all of them except $[1,20]$ and $[22,36]$ are located in the corridor. Note that here, $p+3=21$ (see positions $[1,36]$ and $[20,22]$).

Two regions within the corridor are highlighted by borders drawn around them; they consist of 15 positions each, and their shape and content are identical. We call them *butterflies*. Observe that both ends of the undefined zone are delimited with a butterfly.

Loops defined by completing this template have two useful properties; we proceed with their statements and proofs.

Lemma 2.1. *If a loop has a Cayley table consistent with the template and if it also satisfies the constraint that $[i,j] \neq 0$ in every position where $i+j=n$, then it is subloop-free.*

Proof: Let $k \in G$ and let $\langle k \rangle$ denote the subloop it generates; we show that $\langle k \rangle = G$ for every $k \neq 0$. We first consider $k=2$: it is readily seen from the above specifications that $[2,j] = j+2$ for every $2 \leq j \leq n-3$, which implies that 2 generates all even values between 2 and $n-1$. Next, $[2,n-1]=3$, and from this all odd values between 5 and $n-2$ can be generated. Finally, $[2,n-2]=1$ and $[2,1]=0$ yield $\langle 2 \rangle = G$. Next, since $[1,1]=2$, it follows that $\langle 1 \rangle = G$. Reasoning as in the case $k=2$, it is easily verified that $\langle k \rangle = G$ for $3 \leq k \leq 7$.

In the center of the template we observe $[p+1,p+1]=3$, $[p+2,p+2]=5$, $[p+3,p+3]=1$, $[p+4,p+4]=7$; therefore, $\langle p+1 \rangle = \langle p+2 \rangle = \langle p+3 \rangle = \langle p+4 \rangle = G$.

Next, $\langle n-1 \rangle = G$ follows from the observation that $[n,j] = j-1$ for every $p+5 \leq j \leq n-1$, therefore $p+4 \in \langle n-1 \rangle$. Also, since $[p,p] = n-1$, we have $\langle p \rangle = G$.

We deal with the other $k \in G$ by induction. Since $[k,k] < k$ for every $k \geq p+4$, we only have to consider the case $8 \leq k \leq p-1$. For every such k and every $1 \leq j \leq n-k-1$ we have $[k,j] = k+j$, so that we know that every $tk+j \leq n-1$ belongs to $\langle k \rangle$ as soon as we have verified that $j \in \langle k \rangle$. If n is a multiple of k, then we apply this to $j=k$ and $t = n/k - 1$; the entry $[k,n-k]$ is subject to the condition of the lemma's statement, which yields $[k,n-k] \in \{1,2,3,4,5\}$. Otherwise k does not divide n, i.e. $n = (s+1)k - t$ with $0 < t < k$. We are done if $[k,sk]$ is nonzero. Otherwise the entry $[k,sk]=0$ is in the corridor, which means $n \leq k + sk \leq n+5$. Since the entries $[k,n-k], \ldots, [k,n-1]$ are a permutation of $\{0,\ldots,k-1\}$, it suffices to show that there is at least one $\ell \in \langle k \rangle$ such that $n-k \leq \ell \leq n-1$ and $\ell \neq sk$. Since $k \leq p-1$ and $n = 2p+1$, we have $s > 1$ and $n < 2sk < 2n$. Therefore $[sk,sk] = 2sk \ (mod\ n) = tk+j$ for some $0 < j < k$. By the above reasoning, we can take $\ell = rk + j$ for an appropriate $r \geq t$. □

Lemma 2.2. *If the Cayley table of an order-n loop G is consistent with the template, then $\mathcal{A}_n$ is a subgroup of $\mathcal{M}(G)$.*

Proof: By definition, $\mathcal{M}(G)$ is a transitive permutation group, and it is easily verified that the absence of a nontrivial subloop in G implies that $\mathcal{M}(G)$ is primitive. By a theorem of Jordan (see [18, Theorem 13.9]), $\mathcal{A}_n$ is a subgroup of any primitive group of degree n which contains a 3-cycle. Let G be a loop as

$$L_2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & \cdots & n-4 & n-3 & n-2 & n-1 \\ 2 & 0 & 4 & 5 & 6 & \cdots & n-2 & n-1 & 1 & 3 \end{pmatrix}$$
$$L_3 = \begin{pmatrix} 0 & 1 & 2 & 3 & \cdots & n-5 & n-4 & n-3 & n-2 & n-1 \\ 3 & 4 & 5 & 6 & \cdots & n-2 & n-1 & 1 & 2 & 0 \end{pmatrix}$$

FIGURE 2. Permutations L_2 and L_3

in the lemma's statement. Consider the left translations L_2 and L_3 of 2 and 3, respectively; they are totally defined by the template and are depicted, in matrix notation, on Figure 2. The reader can verify that both permutations consist of a unique cycle of length n, that $L_2(x) = x + 2$ for all $x \notin \{1, n-2, n-1\}$, and that $L_3(x) = x + 3$ for all $x \notin \{n-3, n-2, n-1\}$. The permutations $\alpha = L_2 \circ L_3$ and $\beta = L_3 \circ L_2$ differ only on elements 2, 3 and 6, and $\alpha^{-1} \circ \beta = (2\ 3\ 6)$. □

Finally, we give a criterion to decide whether the translation of a loop element is an even permutation.

Lemma 2.3. *For every $i \in \{6, \ldots, n-2\}$ other than $p+2$ and $p+4$, the translation L_i is an even permutation iff the table entries $[i, n-i]$ to $[i, n-i+5]$ constitute an even permutation of $\{0, 1, 2, 3, 4, 5\}$.*

PROOF: Consider the translation L_i, $i \in \{6, \ldots, n-2\} \setminus \{p+2, p+4\}$. Taking its composition with the mapping $x \mapsto x - i \ (mod\ n)$, which is an even permutation, yields a permutation with fixed points everywhere except in the set $\{n-i, n-i+1, \ldots, n-i+5\}$. □

The translations not covered by this lemma are fully specified by the template. Verifying that they have even parity is done for L_4 and L_5 by the above reasoning; meanwhile, L_2 and L_3 consist of a unique cycle of odd length, and L_1 consists of a 3-cycle and two other cycles of equal parity. Reasoning as above shows that the compositions $(5\ \ p+3) \circ L_{n-1}$, $(3\ \ p+3) \circ L_{p+2}$ and $(5\ \ p+3) \circ L_{p+4}$ are odd permutations.

To complete the proof of the theorem, it suffices to show how to fill each line and column of the undefined zone with an even permutation of $\{0, 1, 2, 3, 4, 5\}$, while respecting the condition that $[i, n-i] \neq 0$ for all $i \neq 0$. For this we define a special type of patterns which we call *blocks*. A block of index m is an array of $6(m+1) + 9$ cells located on six consecutive antidiagonals; there are $m + 1$ complete rows (six cells each) and 9 cells placed on 5 incomplete rows. Every entry is defined, every complete row and column is an even permutation of $\{0, 1, 2, 3, 4, 5\}$, and the ends of this array constitute two disjoint copies of the butterfly. Two blocks can be combined to build a larger block, by making the top right butterfly of one block overlap with the bottom left butterfly of the other, as illustrated in Figure 3. Combining two blocks of orders m and q, respectively, creates a block of order $m + q$.

Thus, filling the template is simply done by inserting a block which fits the undefined zone. Rows 7 to $p-1$ in the table coincide with the $m+1$ fully defined

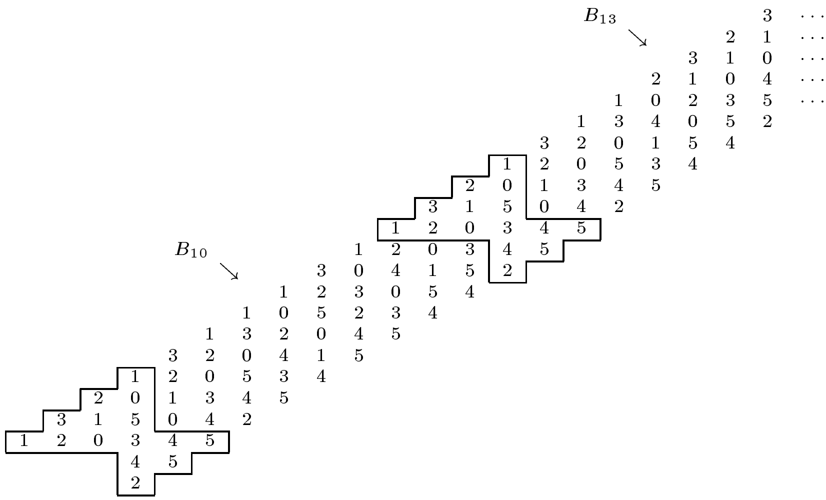

Figure 3. Concatenation of blocks B_{10} and B_{13}

rows in the block, so that its order is $m = p - 8$, or conversely $n = 2m + 17$. Experimentally, we found that the collection of blocks

$$B_{10}, B_{13}, B_{14}, B_{15}, B_{16}, B_{17}, B_{18}, B_{19}, B_{21}, B_{22},$$

depicted on Figure 3 and in the Appendix, enables us to define a loop with $\mathcal{M}(G) = \mathcal{A}_n$ for $n = 37$ (built from B_{10}) and for every odd $n \geq 43$. Each full row and column in these blocks is an even permutation of $\{0, 1, 2, 3, 4, 5\}$. Also, since 0 never occurs at a position $[i, n - i]$, the loops built from these blocks satisfy the condition of Lemma 2.1. In other words, a loop built from the template and our list of blocks is subloop-free, commutative, and such that $\mathcal{M}(G) = \mathcal{A}_n$. □

Corollary 2.4. *For every odd $n \geq 7$, there exists a commutative subloop-free loop G which satisfies $\mathcal{M}(G) = \mathcal{S}_n$.*

Proof: For the smaller values of n, we generated by computer commutative subloop-free loops consistent with the template and observed that the vast majority of them satisfy $\mathcal{M}(G) = \mathcal{S}_n$. For the larger orders, we leave it to the reader to modify the blocks B_{10} to B_{22}, in order to make each of them contain at least one odd permutation of $\{0, 1, 2, 3, 4, 5\}$. □

3. Conclusion

As a preliminary step in this research, we computed $\mathcal{M}(G)$ for all loops of size 6 to 8 using data from [14] and [9], and identified those which were subloop-free. Our results are summarized in Figure 4. Among them, we noticed a loop of size 8 for which $\mathcal{M}(G)$ is neither $\mathcal{S}_n$ nor $\mathcal{A}_n$; this multiplication group has order 1344

Order	Number	Multiplication group			
n	of loops	$\mathcal{S}_n$	$\mathcal{A}_n$	$\mathbb{Z}_n$	Other
5	2	1	0	1	0
6	28	28	0	0	0
7	9 906	9 904	1	1	0
8	43 803 136	43 799 370	3 765	0	1

FIGURE 4. Multiplication group of subloop-free loops, orders 5 to 8

	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	0	5	6	7	4
2	2	4	7	6	1	3	0	5
3	3	6	1	5	2	7	4	0
4	4	0	5	7	6	2	3	1
5	5	7	0	4	3	1	2	6
6	6	5	4	2	7	0	1	3
7	7	3	6	1	0	4	5	2

FIGURE 5. Loop of order 8 with $\mathcal{M}(G) = AL(8)$.

and is denoted $AL(8)$ in the compendium [7]. The Cayley table of this loop is displayed in Figure 5.

The vast majority of nonassociative subloop-free loops of small order satisfy $\mathcal{M}(G) = \mathcal{S}_n$, and it is likely to be the same for every order. In this article, however, we proved that for every odd order $n \geq 7$, there exist a commutative subloop-free loop whose multiplication group is $\mathcal{A}_n$. This result, alongside with the identification of the order-8 loop mentioned above, suggests that subloop-free loops of larger order deserve further investigation.

Acknowledgment. The authors extend their thanks to Markus Holzer, Ian Wanless and an anonymous referee for helpful comments, informations, and suggestions for improvements. This research was supported by NSERC of Canada and FQRNT of Québec.

REFERENCES

[1] Albert A.A., *Quasigroups. I*, Trans. Amer. Math. Soc. **54** (1943), 507–519.

[2] Bruck R.H., *Contributions to the theory of loops*, Trans. Amer. Math. Soc. **60** (1946), 245–354.

[3] Bruck R.H., *A Survey of Binary Systems*, Springer, 1966.

[4] Cameron P.J., *Almost all quasigroups have rank* 2, Discrete Math **106/107** (1992), 111–115.

[5] Cavenagh N.J., Greenhill C., Wanless I.M., *The cycle structure of two rows in a random latin square*, Random Structures Algorithms **33** (2008), 286–309.

[6] Chein O., Pfugfelder H.O., Smith J.D.H., *Quasigroups and Loops: Theory and Applications*, Helderman, Berlin, 1990.

[7] Conway J.H., Hulpke A., McKay J., *On transitive permutation groups*, LMS J. Computer Math. **1** (1998), 1–8.

[8] Drápal A., Kepka T., *Alternating groups and latin squares*, European J. Combin. **10** (1989), 175–180.

[9] Guérin P., *Génération des classes d'isomorphisme des boucles d'ordre* 8, Master Thesis, Université du Québec à Chicoutimi, 2003.

[10] Häggkvist R., Janssen J.C.M., *All-even latin squares*, Discrete Math. **157** (1996), 199–206.

[11] Hall M., *An existence theorem for latin squares*, Bull. Amer. Math. Soc. **51** (1945), 387–388.

[12] Hall M., *The Theory of Groups*, Macmillan, New York, 1959.

[13] Maenhaut B., Wanless I.M., Webb B.S., *Subsquare-free Latin squares of odd order*, European J. Combin. **28** (2007), 322–336.

[14] McKay B.D., Meynert A., Myrvold W., *Small Latin squares, quasigroups, and loops*, J. Combin. Des. **15** (2007), 98–119.

[15] Niemenmaa M., Kepka T., *On multiplication groups of loops*, J. Algebra **135** (1990), 112–122.

[16] Pflugfelder H.O., *Quasigroups and Loops: Introduction*, Heldermann, Berlin, 1990.

[17] Vesanen A., *The group $PSL(2,q)$ is not the multiplication group of a loop*, Comm. Algebra **22** (1994), 1177–1195.

[18] Wielandt H., *Finite Permutation Groups*, Academic Press, New York-London, 1964.

Appendix

Appendix A. Small subloop-free loops

We display in full the Cayley tables of commutative subloop-free loops of orders 7 to 13 such that $\mathcal{M}(G) = \mathcal{A}_n$.

	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	0	4	3	6	5
2	2	0	3	5	6	4	1
3	3	4	5	6	1	2	0
4	4	3	6	1	5	0	2
5	5	6	4	2	0	1	3
6	6	5	1	0	2	3	4

	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	0	4	5	3	7	8	6
2	2	0	6	1	3	7	8	4	5
3	3	4	1	5	7	8	0	6	2
4	4	5	3	7	8	6	1	2	0
5	5	3	7	8	6	1	2	0	4
6	6	7	8	0	1	2	4	5	3
7	7	8	4	6	2	0	5	3	1
8	8	6	5	2	0	4	3	1	7

	0	1	2	3	4	5	6	7	8	9	10
0	0	1	2	3	4	5	6	7	8	9	10
1	1	2	0	4	5	6	3	8	9	10	7
2	2	0	3	7	8	1	5	9	10	4	6
3	3	4	7	8	1	2	9	10	5	6	0
4	4	5	8	1	7	9	10	2	6	0	3
5	5	6	1	2	9	10	8	3	0	7	4
6	6	3	5	9	10	8	4	0	7	2	1
7	7	8	9	10	2	3	0	6	4	1	5
8	8	9	10	5	6	0	7	4	1	3	2
9	9	10	4	6	0	7	2	1	3	5	8
10	10	7	6	0	3	4	1	5	2	8	9

	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	0	4	5	6	7	3	9	10	11	12	8
2	2	0	3	5	6	7	1	9	10	11	12	8	4
3	3	4	5	1	7	9	8	10	11	12	6	2	0
4	4	5	6	7	8	1	10	11	12	3	2	0	9
5	5	6	7	9	1	10	11	12	4	8	0	3	2
6	6	7	1	8	10	11	12	2	5	0	4	9	3
7	7	3	9	10	11	12	2	6	0	4	8	5	1
8	8	9	10	11	12	4	5	0	7	2	3	1	6
9	9	10	11	12	3	8	0	4	2	5	1	6	7
10	10	11	12	6	2	0	4	8	3	1	9	7	5
11	11	12	8	2	0	3	9	5	1	6	7	4	10
12	12	8	4	0	9	2	3	1	6	7	5	10	11

Appendix B. Blocks for loops of large order

In this section, we display the blocks B_{13} to B_{22} used in the proof of the theorem; block B_{10} can be seen on Figure 3. Except for B_{13}, we show only the entries specific to the blocks, i.e. those located between the butterflies. Blocks are represented as arrays where each row corresponds to an antidiagonal in the Cayley table, and each column to a column in the Cayley table. Expressed otherwise: if the entry located at $[a, b]$ in the array is at position $[i, j]$ in the Cayley table, then position $[a, b+1]$ corresponds to $[i-1, j+1]$, and $[a+1, b]$ to $[i+1, j]$.

$\mathbf{B_{13}}$

1	3	2	1	3	1	1	2	3	2	3	1	2	1	3	2	1		
	2	1	0	2	2	3	0	1	1	1	0	0	0	2	1	0		
		0	5	1	0	0	4	2	0	0	5	1	3	1	0	5		
			3	0	3	5	1	0	3	4	2	3	2	4	3	3		
			4	4	4	4	3	5	5	5	3	4	4	5	5	4	4	
			2	5	5	2	5	4	4	2	4	5	5	0	4	2	5	5

$\mathbf{B_{14}}$

3	1	1	1	2	1	1	1	3	1			
2	2	0	3	4	3	3	2	2	0	2		
1	0	5	2	0	0	0	0	0	3	4	0	
0	3	3	0	3	2	2	5	4	5	0	1	3
	4	4	4	1	5	5	3	1	2	3	5	5
		2	5	5	4	4	4	5	4	5	4	4

$\mathbf{B_{15}}$

1	3	2	3	2	2	3	2	3	1	2			
0	2	1	1	1	1	1	1	1	0	0	0		
3	4	0	0	0	0	0	0	0	5	1	3	1	
2	1	3	5	4	3	4	3	4	2	3	2	4	3
	0	5	2	3	5	5	5	5	3	4	4	5	5
		4	4	5	4	2	4	2	4	5	5	0	4

$\mathbf{B_{16}}$

1	1	3	1	1	1	2	1	1	1	3	1			
0	2	5	2	2	3	3	0	3	2	2	0	2		
3	3	0	0	0	0	0	2	5	0	0	3	4	0	
2	4	2	3	3	4	5	4	0	3	4	5	0	1	3
	0	1	4	4	2	1	3	2	4	1	2	3	5	5
		4	5	5	5	4	5	4	5	5	4	5	4	4

$\mathbf{B_{17}}$

1	1	2	1	3	2	2	3	4	1	1	3	1			
0	2	3	3	0	1	1	1	1	0	2	2	0	2		
3	3	0	0	1	4	0	0	0	2	3	0	3	4	0	
2	4	5	4	2	0	3	5	3	3	0	1	5	0	1	3
	0	1	2	5	5	5	2	2	5	5	5	2	3	5	5
		4	5	4	3	4	4	5	4	4	4	4	5	4	4

$\mathbf{B_{18}}$

1	1	2	1	3	2	1	1	3	4	1	1	3	1			
0	2	3	3	0	1	0	0	0	1	0	2	2	0	2		
3	3	0	0	1	4	2	3	2	2	2	3	0	3	4	0	
2	4	5	4	2	0	3	5	1	3	3	0	1	5	1	0	3
	0	1	2	5	5	5	2	4	5	5	5	5	2	3	5	5
		4	5	4	3	4	4	5	0	4	4	4	4	5	4	4

$\mathbf{B_{19}}$

1	1	2	1	1	1	1	3	1	5	2	3	3	1	2			
0	2	3	3	3	2	3	0	2	0	1	1	1	0	0	0		
3	3	0	0	0	0	0	2	3	1	3	0	0	2	1	3	1	
2	4	5	4	2	4	2	4	0	2	0	2	2	4	5	2	4	3
	0	1	2	5	5	5	5	5	4	4	4	4	3	3	4	5	5
		4	5	4	3	4	1	4	3	5	5	5	5	4	5	0	4

$\mathbf{B_{21}}$

3	1	1	1	2	3	1	3	2	3	2	2	3	2	3	1	2			
2	2	3	0	5	1	2	0	1	1	1	1	1	1	1	0	0	0		
1	0	0	2	3	0	0	1	5	0	0	0	0	0	0	5	1	3	1	
0	3	5	4	0	2	3	4	0	2	4	3	4	3	4	2	3	2	4	3
	4	4	3	1	4	4	2	3	4	3	5	5	5	5	3	4	4	5	5
		2	5	4	5	5	5	4	5	5	4	2	4	2	4	5	5	0	4

$\mathbf{B_{22}}$

3	1	1	1	2	1	1	1	3	1	1	1	2	1	1	1	3	1			
2	2	0	3	4	3	3	2	2	0	2	3	3	0	3	2	2	0	2		
1	0	5	2	0	0	0	0	0	3	4	0	0	2	5	0	0	3	4	0	
0	3	3	0	3	2	2	5	4	5	0	2	5	4	0	3	4	5	0	1	3
	4	4	4	1	5	5	3	1	2	3	5	1	3	2	4	1	2	3	5	5
		2	5	5	4	4	4	5	4	5	4	4	5	4	5	5	4	5	4	4

Appendix C. Subloop-free loops of intermediate order

We give examples of commutative subloop-free loops of odd order n, $15 \leq n \leq 41$ and $n \neq 37$, which satisfy $\mathcal{M}(G) = \mathcal{A}_n$. To obtain them, we made an exhaustive search from a template where most of the corridor was left undefined, the rest being identical to the description given in the article. For each order n, we display the upper half of the corridor of one of our results; we represent all entries from the main diagonal (entries printed in boldface) up to and including row 3.

$n = 15$

1	0	3	1	2		
3	2	1	0	3	0	
	5	0	2	1	2	1
	1	2	3	5	4	2
		4	4	4	3	0
		5	10	0	5	4

$n = 17$

1	1	3	2	1	1		
3	2	2	1	0	0	2	
	0	0	0	5	3	3	0
	5	5	3	3	2	4	2
		4	4	4	4	0	1
		1	11	2	5	5	4

$n = 19$

1	0	3	1	2	1	1		
3	2	1	0	3	0	0	2	
	5	0	2	1	2	3	3	0
	1	2	3	5	4	5	4	2
		4	4	4	3	2	0	1
		5	12	0	5	4	5	4

$n = 21$

3	1	0	3	1	2	1	1		
1	2	2	1	0	3	0	0	2	
	0	1	0	2	1	2	3	3	0
	5	5	4	3	5	4	5	4	2
		4	2	5	4	3	2	0	1
		3	13	4	0	5	4	5	4

$n = 23$

1	0	2	4	1	1	2	1	1		
3	2	1	1	3	0	0	3	0	2	
	5	3	3	0	2	3	2	4	0	0
	1	0	0	2	3	1	5	3	3	2
		4	2	5	5	5	0	2	5	1
		5	14	4	4	4	4	5	4	4

$n = 25$

1	1	3	2	5	1	1	2	1	1		
3	2	2	1	1	0	3	3	0	0	2	
	0	0	0	0	3	2	0	2	3	3	0
	5	5	3	3	2	0	1	4	5	4	2
		4	4	4	4	4	4	3	2	0	1
		1	15	2	5	5	5	5	4	5	4

$n = 27$

1	1	2	3	1	1	0	2	2	1	1		
3	2	0	1	0	5	2	1	1	0	0	2	
	0	3	2	3	2	3	3	3	3	3	3	0
	5	5	0	4	0	1	0	0	4	5	4	2
		4	4	5	3	4	4	4	5	2	0	1
		1	16	2	4	5	5	5	2	4	5	4

$n = 29$

1	0	2	4	1	1	2	3	3	2	1	1		
3	2	1	1	3	0	0	1	1	1	0	0	2	
	5	3	3	0	2	3	5	0	0	5	3	3	0
	1	0	0	2	3	1	2	2	4	2	2	4	2
		4	2	5	5	5	0	4	3	3	4	0	1
		5	17	4	4	4	4	5	5	4	5	5	4

$n = 31$

1	1	3	2	5	1	1	1	1	4	2	0	1		
3	2	2	1	1	0	3	2	0	3	1	1	2	2	
	0	0	0	0	3	2	0	3	2	0	3	3	3	0
	5	5	3	3	2	0	3	2	0	3	2	0	0	2
		4	4	4	4	4	4	4	5	5	5	5	5	1
		1	18	2	5	5	5	5	1	4	4	4	4	4

	1	1	3	2	5	1	1	2	1	1	1	2	1	1		
	3	2	2	1	1	0	3	3	4	3	0	5	0	0	2	
$n = 33$		0	0	0	0	3	2	0	0	0	2	3	3	3	3	0
		5	5	3	3	2	0	1	2	2	3	0	2	2	4	2
			4	4	4	4	4	4	3	5	5	1	4	4	0	1
			1	19	2	5	5	5	5	4	4	4	5	5	5	4

	1	1	2	3	1	2	3	3	0	1	1	3	2	1	1		
	3	2	0	1	0	0	1	1	1	4	2	2	1	0	0	2	
$n = 35$		0	3	2	3	1	2	0	2	2	3	0	0	5	3	3	0
		5	5	0	4	5	4	5	3	0	0	1	3	3	2	4	2
			4	4	5	3	0	2	4	5	5	5	5	4	4	0	1
			1	20	2	4	5	4	5	3	4	4	4	2	5	5	4

	1	1	3	2	5	1	3	1	1	3	1	1	2	3	0	2	1		
	3	2	2	1	1	0	2	2	3	2	0	0	0	1	1	1	3	2	
$n = 39$		0	0	0	0	3	1	0	0	0	4	2	3	2	3	5	2	0	0
		5	5	3	3	2	0	3	4	1	2	3	1	5	4	0	0	3	1
			4	4	4	4	4	4	2	5	5	5	5	4	2	3	4	4	4
			1	22	2	5	5	5	5	4	3	4	4	0	5	4	5	5	2

	1	1	3	2	1	1	1	0	1	1	3	0	1	1	3	2	1	1		
	3	2	2	1	0	0	2	3	2	2	0	1	4	2	2	1	0	0	2	
$n = 41$		0	0	0	5	3	3	5	0	3	5	2	2	3	0	0	5	3	3	0
		5	5	3	3	2	4	2	3	4	1	3	3	0	1	3	3	2	4	2
			4	4	4	4	0	1	4	0	2	4	0	5	5	5	4	4	0	1
			1	23	2	5	5	4	5	5	4	5	5	4	4	4	2	5	5	4

Martin Beaudry:
Département d'informatique, Université de Sherbrooke, Sherbrooke, Québec, Canada J1K 2R1

E-mail: martin.beaudry@usherbrooke.ca

Louis Marchand:
Département d'informatique, Université de Sherbrooke, Sherbrooke, Québec, Canada J1K 2R1

(*Received* May 6, 2011, *revised* September 8, 2011)