PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 55 (69), 1994, 1–8

ON SOME CLASSES OF FINITE LOOPS

Dragan M. Acketa and **Snežana Matić-Kekić**

Abstract. Four new equivalence classes of finite loops are considered: C-, R-, E- classes, and parastrophic closures. The first three classes are natural interclasses between isomorphic and isotopy classes of loops. Their internal isotopies are characterized and a way for generating isotopy classes from C-classes and R-classes is pointed to. The exact upper bound for the length of parastrophic closures is determined.

1. Preliminaries

This paper is concerned with some properties of the four new equivalence classes of loops: C-, R-, E- classes, and parastrophic closures, which were introduced in [**1**]. The C-, R- and E-classes are interclasses between isomorphic and isotopy classes of loops; the isotopies within them are characterized in Section 2.1. The mutually dual C- and R-classes are used in Section 2.2 for representing isotopy transformations over $L(n)$ and for a construction of isotopy classes. It turns out that E-classes have a specific behaviour, although their definition is analogous to the definitions of C- and R-classes.

It is known [**3**] that iterative applications of parastrophic operators *within the class of loops* (to a fixed initial loop) produce loops belonging to at most six different isomorphic classes. Parastrophic closures are obtained when the arising loops themselves are considered, instead of their isomorphic classes. The best possible upper bound for the cardinality of parastrophic closure is established in Section 3.

Some necessary definitions and denotations are given in the sequel. Let $S(n)$ denote the set $\{1, \dots, n\}$. A *latin square of order* n [**4**] is an $n \times n$ matrix A with the elements in $S(n)$, which satisfies that there are no two coinciding elements in the same row or in the same column of A. A *loop* (with unit 1) of order n is a latin square of order n which satisfies: $A[i, 1] = A[1, i] = i$, for $1 \leq i \leq n$. $L(n)$ will denote the set of loops of order n. Definitions of six kinds of equivalence classes

Key words and phrases: latin squares, isotopy, isomorphic, C-, R-, E- classes, parastrophic closures.

AMS Subject Classification (1980): Primary 05B15

over $L(n)$ follow: Two loops X and Y of order n belong to the same *isotopy class* if there exists an *isotopy*, i.e., a triple $T=(p,q,r)$ of permutations of $S(n)$ satisfying $Y[p(i),q(j)]=r(X[i,j])$, for$1\leq i,j\leq n$. In particular, if T is of the form (p,p,p), (q,p,p), (p,q,p) or (p,p,q), then the loops X and Y are respectively said to belong to the same *isomorphic class*,C-class,R-class or E-class. The relationships existing among the permutations p and q (in the last three cases) are given in Section 2.1.

Let r_A and l_A respectively denote the permutations of $S(n)$ which produce the right and the left inverse elements of the loop A (thus $A[i,r_A(i)]=1$ and $A[l_A(i),i]=1$ for $i\in S(n)$).

Each loop A has six *loop-parastrophes* A, $\rho(A)$, $\lambda(A)$, $\tau(A)$, $\lambda\tau(A)$, $\rho\tau(A)$, associated to it, where τ is the transposition operator, while the operators ρ and λ have the following meaning (denotations ρ and λ are in accordance with the denotations used in [**3**]: $\rho(A)[r_A(i),A[i,j]]=j$, and $\lambda(A)[A[i,j],l_A(j)]=i$, for $1\leq i,j\leq n$.

Two loops X and Y from $L(n)$ are said to belong to the same *parastrophic closure* if there exists a sequence $X=Z_1,Z_2,\ldots,Z_k=Y$ of loops from $L(n)$, such that Z_{i+1} is a loop-parastroph of Z_i, for $1\leq i\leq k-1$. The parastrophic closure associated to loop A will be denoted by $PC(A)$.

The table [**2**] contains some summary data for $n\leq 6$, including cardinality of $L(n)$, as well as the number of all the considered subclasses of $L(n)$:

n	≤ 3	4	5	6
cardinality of $L(n)$	1	4	56	9408
number of isomorphic classes in $L(n)$	1	2	6	109
number of E-classes in $L(n)$	1	2	5	103
number of C-(also number of R-) classes in $L(n)$	1	2	3	40
number of isotopy classes in $L(n)$	1	2	2	22
number of parastrophic closures in $L(n)$	1	4	14	832

The *order* O of a permutation p is the smallest natural number such that p^O is the identical permutation.

2. C-, R- and E-classes

2.1. Relationships between permutations p and q in the definitions of C-, R- and E-classes. The three lemmae of this section establish the relationships between the permutations p and q used in the definitions of C-, R- and E-classes. More precisely, given a permutation p of $S(n)$, we shall characterize the permutations q of $S(n)$, such that the isotopies (q,p,p), (p,q,p), and (p,p,q) map $L(n)$ to $L(n)$. It turns out that the permutation p in the third case is not arbitrary.

LEMMA 1. *An isotopy (q,p,p) maps a loop X from $L(n)$ to another loop in $L(n)$ if and only if $q(i)=p(X[i,p^{-1}(1)])$, for $1\leq i\leq n$.*

Proof. Let Y denote the image of X under the isotopy (q,p,p). Then $Y[i,j] = p(X[q^{-1}(i), p^{-1}(j)])$, for $1 \leq i,j \leq n$.

only-if part: Since $Y \in L(n)$, then $q(i) = Y[q(i),1] = p(X[i,p^{-1}(1)])$, for $1 \leq i \leq n$.

if part: Let $q(i) = p(X[i,p^{-1}(1)])$, for $1 \leq i \leq n$, where $X \in L(n)$. We are going to show that the image Y has the element 1 as both the left and the right unit.

Y has the left unit 1: Note primarily that $q(1) = p(X[1,p^{-1}(1)]) = p(p^{-1}(1)) = 1$. It further follows that for $1 \leq j \leq n$:

$$Y[1,j] = p(X[q^{-1}(1), p^{-1}(j)]) = p(X[1,p^{-1}(j)]) = p(p^{-1}(j)) = j.$$

Y has the right unit 1: Similarly as in the only-if part

$$Y[q(i),1] = p(X[i,p^{-1}(1)]) = q(i), \text{ for } 1 \leq i \leq n. \quad \square$$

LEMMA 2. *An isotopy (p,q,p) maps a loop X from $L(n)$ to another loop in $L(n)$ if and only if $q(i) = p(X[p^{-1}(1),i])$, for $1 \leq i \leq n$.*

Proof. Dual to the previous one; the roles of rows and columns are interchanged. $\square$

The definition of E-classes is analogous to the definitions of C- and R-classes w.r.t. the concept of general isotopy. However, when the consideration is restricted to the loops in $L(n)$, it turns out that E-classes have a special role.

LEMMA 3. *An isotopy (p,p,q) maps a loop X from $L(n)$ to another loop in $L(n)$ if and only if $q(X[p^{-1}(1),i]) = q(X[i,p^{-1}(1)]) = p(i)$, for $1 \leq i \leq n$.*

Proof. Let Y denote the image of X under the isotopy (p,p,q). Then

$$Y[i,j] = q(X[p^{-1}(i), p^{-1}(j)]), \text{ for } 1 \leq i,j \leq n.$$

only-if part: Since $Y \in L(n)$, then $p(i) = Y[p(i),1] = q(X[i,p^{-1}(1)])$, and $p(i) = Y[1,p(i)] = q(X[p^{-1}(1),i])$, for $1 \leq i \leq n$.

if part: The element 1 is proved to be both the left and the right unit of Y: $Y[p(i),1] = q(X[i,p^{-1}(1)]) = p(i)$, and $Y[1,p(i)] = q(X[p^{-1}(1),i]) = p(i)$, for $1 \leq i \leq n$. $\square$

Remark. The *commutator* of a loop $X \in L(n)$ is the set of those elements $k \in S(n)$, satisfying $X[k,j] = X[j,k]$, for each $j \in S(n)$. The element $p^{-1}(1)$ in the previous lemma belongs to the commutator of X. It turns out that the element 1 belongs to the commutator of the image Y of the loop X under the isotopy (p,p,q), since $X[p^{-1}(1),i] = X[i,p^{-1}(1)]$ implies $q(X[p^{-1}(1),p^{-1}p(i)]) = q(X[p^{-1}p(i),p^{-1}(1)])$ and $Y[1,p(i)] = Y[p(i),1]$.

It can be proved in a similar way that each element k of the commutator of X is mapped by the isotopy (p,p,q) to the element $p(k)$ of the commutator of Y. It follows that those isotopies of the form (p, p, q), which map $L(n)$ to $L(n)$, preserve the cardinality of the commutator.

Consequently, an abridged search for E-classes can be gained by partitioning (representatives of) isomorphic classes w.r.t. this cardinality. If the commutator of a loop is equal to $\{1\}$, then its isomorphic class coincides with its E-class (since $p(1) = 1$ implies $q = p$).

2.2. Generating isotopy classes over $L(n)$ from C-classes and R-classes. A property of isotopies over the class $L(n)$ is described by the following lemma (which is an easy consequence of Lemmae 1.1 and 1.2 from [**3**]):

LEMMA 4. *Each isotopy (p, q, r), which maps a loop X from $L(n)$ to another loop in $L(n)$, satisfies $p(i) = r(X[i, m])$ and $q(i) = r(X[l, i])$, for $1 \le i \le n$, for some index pair (l, m), which satisfies $r(X[l, m]) = 1$.*

Proof. If $m = q^{-1}(1)$ and $l = p^{-1}(1)$, then for $1 \le i \le n$, $p(i) = Y[p(i), 1] = r(X[i, q^{-1}(1)]) = r(X[i, m])$ and $q(i) = Y[1, q(i)] = r(X[p^{-1}(1), i]) = r(X[l, i])$. $\square$

The following lemma says that the general isotopy transformation over $L(n)$ can be represented as a product of two special isotopy transformations, one of which is restricted to an C-class, while the other one is restricted to an R-class:

LEMMA 5. *If two loops X and Z in $L(n)$ are isotopic, then there exists a third loop Y in $L(n)$, such that the loops X and Y belong to the same C-class, while the loops Y and Z belong to the same R-class.*

Proof. Let (p, q, r) be an isotopy mapping X to Z. Further, let p_1 denote an arbitrary permutation of $S(n)$ satisfying $p_1(m) = 1$, where m denotes the index used in Lemma 4. It suffices to prove that there exist permutations p_2, q_1 and q_2 of $S(n)$ and a loop Y in $L(n)$ so that the isotopy (q_1, p_1, p_1) maps X to Y and that the isotopy (p_2, q_2, p_2) maps Y to Z. The equations $q_1 \cdot p_2 = p$, $p_1 \cdot q_2 = q$ and $p_1 \cdot p_2 = r$ imply that $q_2 = p_1^{-1} \cdot q$, $p_2 = p_1^{-1} \cdot r$ and $q_1 = p \cdot r^{-1} \cdot p_1$.

The following derivation

$$q_1(i) = p_1(r^{-1}(p(i))) \overset{\text{Lemma 4}}{=} p_1(r^{-1}(r(X[i, m]))) = p_1(X[i, p_1^{-1}(1)]),$$

for $1 \le i \le n$, combined with Lemma 1, proves that the image Y of the loop X under the isotopy (q_1, p_1, p_1) is a loop in $L(n)$. $\square$

Remark. Notice that there are $(n-1)!$ possible choices for the permutation p_1 and the same number of representations of an isotopy over $L(n)$ in the form of the desired product. Two particular possibilities for p_1 are $p_1 = q$ and $p_1 = r \cdot p^{-1}$.

COROLLARY. *Each C-class has a nonempty intersection with each R-class inside the same isotopy class.*

Proof. Suppose that there exists a C-class C_0 and an R-class R_0 within the same isotopy class so that $C_0 \cap R_0 = \emptyset$. Let the loops X and Z satisfy $X \in C_0$ and $Z \in R_0$. Lemma 5 gives that there exists a loop Y such that the loops X and

Y are in the same C-class (i.e., in the class C_0) and Y and Z are in same R-class (the class R_0). The existence of the loop Y contradicts the assumption. □

C-classes and R-classes can be constructed in a similar way as the isomorphic classes over $L(n)$, by the procedure described in [**1**]. The following Theorem 1 may serve as a basis of an improved algorithm for the construction of isotopy classes over $L(n)$ by using C- and R-classes:

THEOREM 1. *The isotopy classes of loops in $L(n)$ can be determined as the unions of those R-classes which have nonempty intersections with the same C-class.*

Proof. The theorem easily follows from Lemma 5 and its consequence. □

The basic procedure of the construction of isotopy classes over $L(n)$ from C-classes and R-classes detects whether the intersection of a given C-class and a given R-class is empty or not. There are two alternative classes of objects which can be searched for in the course of this procedure: a) common loops, and b) common isomorphic subclasses. It seems that the approach a) is a more efficient, since it does not require the construction of isomorphic classes.

3. On the cardinality of parastrophic closures

A well-known statement from [**3**] says:

STATEMENT. *Iterative applications of loop-parastrophic operators to an initial loop A give loops from at most six different isomorphic classes.*

The six loop-parastrophes of A are the representatives of these six isomorphic classes (it was shown in [**3**] that the loop $\tau(A)$ is isomorphic to each of the loops $\rho\lambda\rho(A)$ and $\lambda\rho\lambda(A)$).

When considering parastrophic closures, we are interested in loops themselves, not merely in their isomorphic classes. It turns out that the generation of the parastrophic closure $PC(A)$, associated to a loop A, often requires longer alternative applications of the operators ρ and λ, which should in some cases be accompanied by one application of the operator τ.

The following theorem, which is the main result of this section, is an analogue of the above statement, when nonisomorphic loops are replaced by non-identical loops:

THEOREM 2. $|PC(A)| \leq 6\,\mathrm{order}(r_A)$ *for each loop A.*

The proof this theorem is based on a number of lemmas.

The definition of loop-parastrophies immediately gives:

LEMMA 6. *All the loops from $PC(A)$ can be obtained by iterative applications of loop-parastrophies ρ, λ and τ to A.*

LEMMA 7. [**3**] $l_A = r_A^{-1}$, $r_A = l_A^{-1}$, $l_{\rho(A)} = r_A$, $r_{\rho(A)} = l_A$, $l_{\lambda(A)} = r_A$, $r_{\lambda(A)} = l_A$, $l_{\tau(A)} = r_A$, $r_{\tau(A)} = l_A$.

LEMMA 8.[**3**] *If a loop A is given, then* (a) $\rho^2(A) = A$ *and* (b) $\lambda^2(A) = A$.

LEMMA 9. *If a loop A is given then* (a) $\rho\tau(A) = \tau\lambda(A)$; (b) $\lambda\tau(A) = \tau\rho(A)$.

Proof. (a) Since $A[i,j] = \tau A[j,i]$ the loops $\rho\tau(A)$ and $\tau\lambda(A)$ satisfy $\rho\tau(A)[r_{\tau(A)}(j), A[i,j]] = i$ and $\tau\lambda(A)[l_A(j), A[i,j]] = i$ respectively. The equality $r_{\tau(A)} = l_A$ from Lemma 7 completes the proof. □

COROLLARY. $\tau(\rho\lambda)^k = (\lambda\rho)^k\tau$ and $\tau(\lambda\rho)^k\lambda = (\rho\lambda)^k\rho\tau$ for $k > 0$.

LEMMA 10. *Given a loop A of order n, the loop $(\lambda\rho)^3(A)$ satisfies*

$$(\lambda\rho)^3(A)[r_A^2(i), r_A^2(j)] = r_A^2(A[i,j]), \text{ for } 1 \le i,j \le n.$$

Proof. Given a loop B, notice that value $= B[$ row_index, column_index$]$ implies

$$\begin{aligned} \text{row\_index} &= \lambda(B)[\text{value}, l_B(\text{column\_index})] \\ \text{column\_index} &= \rho(B)[r_B(\text{row\_index}), \text{value}] \end{aligned}$$

Applying this rule six times, as well as the reduction (by Lemma 7)

$$r_{\lambda\rho\lambda\rho\lambda\rho(A)} = l_{\rho\lambda\rho\lambda\rho(A)} = r_{\lambda\rho\lambda\rho(A)} = l_{\rho\lambda\rho(A)} = r_{\lambda\rho(A)} = l_{\rho(A)} = r_A,$$

it can be iteratively derived that for $1 \le i,j \le n$

$$\begin{gathered} \rho(A)[r_A(i), A[i,j]] = j, \\ \lambda\rho(A)[j, l_{\rho(A)}(A[i,j])] = \lambda\rho(A)[j, r_A(A[i,j])] = r_A(i), \\ \rho\lambda\rho(A)[r_{\lambda\rho(A)}(j), r_A(i)] = \rho\lambda\rho(A)[r_A(j), r_A(i)] = r_A(A[i,j]), \\ \lambda\rho\lambda\rho(A)[r_A(A[i,j]), l_{\rho\lambda\rho(A)}(r_A(i))] = \lambda\rho\lambda\rho(A)[r_A(A[i,j]), r_A^2(i)] = r_A(j), \\ \rho\lambda\rho\lambda\rho(A)[r_{\lambda\rho\lambda\rho(A)}(r_A(A[i,j])), r_A(j)] = \rho\lambda\rho\lambda\rho(A)[r_A^2(A[i,j]), r_A(j)] = r_A^2(i), \\ \lambda\rho\lambda\rho\lambda\rho(A)[r_A^2(i), l_{\rho\lambda\rho\lambda\rho(A)}(r_A(j))] = \lambda\rho\lambda\rho\lambda\rho(A)[r_A^2(i), r_A^2(j)] = r_A^2(A[i,j]). \quad \square \end{gathered}$$

COROLLARY. *If O denotes the order of the permutation r_A, then the operator $(\lambda\rho)^{3O}$ is identity. This further implies that $(\rho\lambda)^i = (\lambda\rho)^{3O-i}$ and $\lambda(\rho\lambda)^i = \rho(\lambda\rho)^{3O-i-1}$ holds for $1 \le i \le 3O-1$.* □

LEMMA 11. *Given a loop A of order n, the loop $(\rho\lambda)^3(A)$ for $1 \le i,j \le n$ satisfies $(\rho\lambda)^3(A)[l_A^2(i), l_A^2(j)] = l_A^2(A[i,j])$,.*

Proof. Dual to the previous one. □

LEMMA 12. *Each loop from $PC(A)$ can always be obtained from A by application of the transformations of the form*

(a) $(\lambda\rho)^i$ *or* $\rho(\lambda\rho)^{i-1}$ *for some $i > 0$ when the order of r_A is odd*

(b) $(\lambda\rho)^i or \rho(\lambda\rho)^{i-1}$ *or* $(\lambda\rho)^i\tau or \rho(\lambda\rho)^{i-1}\tau$ *for some $i > 0$ when the order of r_A is even.*

Proof. It follows from Lemma 8 that two same operators from the set $\{\lambda, \rho, \tau\}$ should be never successively applied, while Consequence of Lemma 10 implies that a product of operators ρ and λ beginning with λ can be always replaced by such a product beginning with ρ.

Lemma 9 implies that the operator τ possesses a kind of commutativity with respect to the operators λ and ρ. This implies that the calls of τ can always be applied first. Thus odd number of appearances of τ can always be reduced to one (which would be applied in the very beginning) and even number can always be reduced to zero.

It remains to show that the odd order of r_A guarantees that the operator τ can be expressed by means of ρ and λ. More precisely: If $\mathrm{order}(r_A) = 2k+1$, then $\tau(A) = (\rho\lambda)^{3(k+1)}(\rho\lambda\rho)(A)$.

Namely, the loop $\rho\lambda\rho(A)$ in the proof of Lemma 10 satisfies

$$\rho\lambda\rho(A)[r_A(j), r_A(i)] = r_A(A[i,j])$$

i.e. (by Lemma 7)

$$\rho\lambda\rho(A)[l_A^{-1}(j), l_A^{-1}(i)] = l_A^{-1}(A[i,j]).$$

If the operator $(\rho\lambda)^{3(k+1)}$ is applied to this loop, then the Lemma 11 gives (since $r_A^{2k+1} = l_A^{2k+1} = \text{identity}$) that the new loop $B = (\rho\lambda)^{3(k+1)}(\rho\lambda\rho)(A)$ satisfies:

$$B[l_A^{2k+2}(l_A^{-1}(j)), l_A^{2k+2}(l_A^{-1}(i))] = l_A^{2k+2}(l_A^{-1}(A[i,j])); \text{ i.e. } B[j,i] = A[i,j]. \quad \square$$

Proof of Theorem. Let O denote the order of permutation r_A. We distinguish two cases, depending on parity of O:

Case 1. O is odd: Lemma 10 implies that $(\lambda\rho)^{3O}(A)[r_A^{2O}(i), r_A^{2O}(j)] = r_A^{2O}(A[i,j])$. The permutation r_A^{2O} is identical, so the loop $(\lambda\rho)^{3O}(A)$ coincides with A. On the other hand, Lemma 12 (a) guarantees that all the loops of $PC(A)$ can be found among the loops $\rho(A)$, $\lambda\rho(A)$, $\ldots$, $(\lambda\rho)^{3O}(A)$. This implies that $|PC(A)| \le 2 \cdot 3 \cdot O$.

Case 2. O is even: Similarly, Lemma 10 implies that

$$(\lambda\rho)^{3O/2}(A)[r_A^O(i), r_A^O(j)] = r_A^O(A[i,j]).$$

The loop $(\lambda\rho)^{3O/2}(A)$ coincides with A. This time Lemma 12(b) guarantees that only half of the loops of $PC(A)$ can be found among the loops $\rho(A), \lambda\rho(A), \ldots,$ $(\lambda\rho)^{3O}(A)$; a loop from the other half can be obtained by putting $\tau(A)$ instead of A in the above sequence. Thus the total number of loops in $|PC(A)|$ cannot be greater than $2 \cdot 2 \cdot \frac{3}{2} \cdot O$. $\square$

COROLLARY: *If A is a loop of order n, then $|PC(A)| \le 6\max F(p)$, where $F(p)$ denotes the least common multiplier of the summands of a partition p, while the maximum is taken over all the partitions p of the number $n-1$.*

Namely, the summands of the partition are associated to the cycle lengths of a permutation p on $S(n)$, which has the fixed point 1.

Remarks. We have made a number of tests with randomly generated loops on $n \geq 7$. Each test has generated 1000 loops A, such that the permutation $r_A = p$ was fixed and given in advance. It turned out that all the generated loops A satisfied $|PC(A)| = 6\,\mathrm{order}(p)$, that is, all of them reached the upper bound of Theorem 2. We therefore conjecture that the length of the parastrophic closure of A of a larger order almost always coincides with $6\,\mathrm{order}(r_A)$.

On the other hand, among all the 9408 loops of order 6 [**2**], only 5650 reach this upper bound. More precisely, the upper bound is reached with all those loops A of order 6, which satisfy $|PC(A)| > 12$, and only with 150 loops with smaller $|PC(A)|$ (120 with $|PC(A)| = 12$ and 30 with $|PC(A)| = 6$). These data motivate the second (general) conjecture:

If $|PC(A)| > 12$ for a loop A, then $|PC(A)| = 6\ \mathrm{order}(r_A)$.

It seems that the loops A of order 6 with $|PC(A)| = 10$ are particularly interesting. All of them have order $(r_A) = 5$. In addition, 10 is the largest length that we know of a alternative product P of operators λ and ρ (beginning with ρ) which satisfies: P is a minimal non-empty such product which fixes the initial loop A and the length of P is less than the theoretical maximum $6\,\mathrm{order}(r_A)$.

The minimal length of a parastrophic closure is settled by the following:

STATEMENT. *For each n there is a loop A of order n so that $|PC(A)| = 1$.*

The multiplication table of the cyclic group on $S(n)$ satisfies the condition of the statement. If $n = 2k$, then another interesting representative of the same isomorphic class of loops can be obtained from the cyclic group on k elements by supstituting each element v in the table by the 2×2 latin square with the elements $2v - 1$ on the main diagonal and the elements $2v$ on the other diagonal.

REFERENCES

1. D.M. Acketa, S. Matić-Kekić, *An algorithm for generating finite loops, some of their subclasses and parastrophic closures,* in: *Proceedings of the 13th ITI-91,* (1991), 549–554.
2. D.M. Acketa, S. Matić-Kekić, *A classification of loops on at most six elements*, submitted.
3. V.D. Belousov, *Osnovi teorii kvazigrup i lup*, Nauka, Moskva, 1967, (in Russian).
4. J. Dénes, A.D. Keedwell, *Latin Squares and their Applications*, Akadémiai Kiadó, Budapest; English Universities Press, London; Academic Press, New York, 1974.

Institut za matematiku
Trg Dositeja Obradovića 4
21000 Novi Sad
Yugoslavia

(Received 08 12 1992)
(Revised 22 05 1994)