LMS J. Comput. Math. 14 (2011) 200–213 © 2011 Authors
doi:10.1112/S1461157010000173

Searching for small simple automorphic loops

Kenneth W. Johnson, Michael K. Kinyon, Gábor P. Nagy and Petr Vojtěchovský

Abstract

A loop is (right) automorphic if all its (right) inner mappings are automorphisms. Using the classification of primitive groups of small degrees, we show that there is no non-associative simple commutative automorphic loop of order less than 2^{12}, and no non-associative simple automorphic loop of order less than 2500. We obtain numerous examples of non-associative simple right automorphic loops. We also prove that every automorphic loop has the antiautomorphic inverse property, and that a right automorphic loop is automorphic if and only if its conjugations are automorphisms.

1. *Introduction*

For a groupoid Q and $x \in Q$, define the *right translation* $R_x : Q \to Q$ by $yR_x = yx$, and the *left translation* $L_x : Q \to Q$ by $yL_x = xy$. A *loop* is a groupoid Q with neutral element 1 in which all translations are bijections of Q.

The *right multiplication group* $\mathrm{Mlt}_\rho(Q)$ of Q is the permutation group generated by all right translations of Q. The *multiplication group* $\mathrm{Mlt}(Q)$ of Q is the permutation group generated by all translations of Q. The *right inner mapping group* $\mathrm{Inn}_\rho(Q)$ of Q is the stabilizer of 1 in $\mathrm{Mlt}_\rho(Q)$. Equivalently, $\mathrm{Inn}_\rho(Q)$ is generated by all *right inner mappings* $R_{x,y} = R_x R_y R_{xy}^{-1}$. The *inner mapping group* $\mathrm{Inn}(Q)$ of Q is the stabilizer of 1 in $\mathrm{Mlt}(Q)$. Equivalently, $\mathrm{Inn}(Q)$ is generated by all right inner mappings, all *left inner mappings* $L_{x,y} = L_x L_y L_{yx}^{-1}$ and all *middle inner mappings* (*conjugations*) $T_x = R_x L_x^{-1}$.

Let $\mathrm{Aut}(Q)$ be the automorphism group of a loop Q. Then Q is a *right automorphic loop* (also known as A_r*-loop*) if $\mathrm{Inn}_\rho(Q) \leqslant \mathrm{Aut}(Q)$, and an *automorphic loop* (also known as *A-loop*) if $\mathrm{Inn}(Q) \leqslant \mathrm{Aut}(Q)$. Note that every group is an automorphic loop, but the converse is certainly not true.

A non-empty subset S of a loop Q is a *subloop* of Q if it is invariant under $\{R_x^\varepsilon, L_x^\varepsilon; x \in S, \varepsilon = \pm 1\}$. A *normal subloop* of Q is a subloop invariant under $\mathrm{Inn}(Q)$, and Q is *simple* if it possesses no normal subloops except for the trivial subloops Q and $\{1\}$.

For an introduction to the theory of loops, see [5].

1.1. *Simple automorphic loops*

Automorphic loops were for the first time studied by Bruck and Paige [6]. The foundations of the theory of commutative automorphic loops were laid by Jedlička *et al.* [19], with such structural results such as the Cauchy theorem, Lagrange theorem, odd order theorem, etc. A paper analogous to [19], but without the assumption of commutativity, is in preparation [21].

By [19, Theorems 5.1, 5.3, 7.1], every finite commutative automorphic loop is a direct product of a solvable loop of odd order and a loop of order a power of two. By [19, Proposition 6.1, Theorem 6.2], a finite simple commutative automorphic loop is either a cyclic group of prime order, or a loop of exponent two and order a power of two. It was shown in [18], by an exhaustive search with a finite model builder, that there are no simple non-associative commutative automorphic loops of order less than 32.

Received 25 May 2010; revised 31 December 2010.

2000 Mathematics Subject Classification 20N05, 20B15 (primary), 20B40 (secondary).

G. P. Nagy was supported by the TAMOP-4.2.1/B-09/1/KONV-2010-0005 project.

By [21], a non-associative finite simple automorphic loop must be of even order.

No examples of non-associative simple automorphic loops are known, and the theory of automorphic loops is not yet sufficiently developed to rule out such examples. In this paper, we use the classification of primitive groups of small degrees to show the following results computationally.

THEOREM 1.1. *There is no non-associative simple commutative automorphic loop of order less than* 2^{12}. *In particular, if* Q *is a finite commutative automorphic loop whose order is not divisible by* 2^{12} *then* Q *is solvable.*

THEOREM 1.2. *There is no non-associative simple automorphic loop of order less than* 2500.

In contrast, there are some examples of non-associative finite simple right automorphic loops in the literature, mostly due to their connection to right Bruck loops and right conjugacy closed loops.

Recall that a loop is a *right Bol loop* if it satisfies the identity $((zx)y)x = z((xy)x)$. The two-sided inverse x^{-1} of an element x is well defined in right Bol loops, and a right Bol loop is a *right Bruck loop* (also known as *right K-loop* or *right gyrocommutative gyrogroup*) if it satisfies the identity $(xy)^{-1} = x^{-1}y^{-1}$. Funk and Nagy showed, using geometric loop theory, that a right Bruck loop is a right automorphic loop [13, Corollary 5.2]. (For an algebraic proof of the same result, see [16] or [22]. For an introduction to Bruck loops, see [20].)

The first example (belonging to an infinite class of examples) of a non-associative finite simple right Bruck loop was constructed in 2007 by Nagy [24], a loop of order 96 and exponent 2. The same example and another non-associative simple right Bruck loop of order 96 (and exponent 4) were found independently by Baumeister and Stein [4]. Both [4, 24] built upon the work of Aschbacher [2].

A loop Q is *right conjugacy closed* if $R_x^{-1}R_yR_x$ is a right translation for every x, $y \in Q$. Every right conjugacy closed loop is right automorphic, by [15]. There are unpublished and easily constructible examples of non-associative simple right conjugacy closed loops of order 8.

As a byproduct of our search for small simple automorphic loops, we obtain a class of non-associative finite simple right automorphic loops. We know, however, that this class does not account for all non-associative finite simple right automorphic loops; notably, it does not contain any of the two simple right Bruck loops of order 96 mentioned above.

1.2. *Open problems*

The following problems remain open.

PROBLEM 1.3. Is there a non-associative finite simple commutative automorphic loop?

Thanks to the decomposition theorem and odd order theorem for finite commutative automorphic loops, cf. [19], Problem 1.3 has a negative answer if and only if every finite commutative automorphic loop is solvable.

PROBLEM 1.4. Is there a non-associative finite simple automorphic loop?

1.3. *Summary of content*

In Section 2 we recall the standard construction of Baer that embeds loops into groups by means of group transversals. Section 3 contains the well known fact that a loop is simple if and only if its multiplication group is primitive, and some information about the available libraries of primitive groups. Necessary and sufficient conditions on right translations that characterize automorphic loops are given in Section 4. These conditions are used in Section 5, where we present an algorithm that, given a transitive group G on Q, finds all right automorphic loops $Q = (Q, *)$ such that $\mathrm{Mlt}_\rho(Q) \leqslant G$ and $G_1 \leqslant \mathrm{Aut}(Q)$. The algorithm is further discussed

in Section 6, where we also establish Theorems 1.1 and 1.2. Of independent interest is the fact that a right automorphic loop is automorphic if and only if all its conjugations are automorphisms, which we prove in Section 7. As is shown in Section 8, certain orders of Theorem 1.1 can be handled theoretically, without the algorithm of Section 5, by using known results on possible multiplication groups of loops, and from the knowledge of conjugacy classes of G_1, where G is a primitive permutation group of affine type. We conclude the paper with a reformulation of Problem 1.3 entirely into group theory.

2. *Loop folders in searches*

It is well known since the work of Baer [3] that every loop can be represented as a transversal in a permutation group. Since our search is based on this fact, we summarize some of his and related results here for the convenience of the reader. (See also [2].)

For a loop Q on $\{1, \ldots, d\}$, let $\mathcal{F}(Q) = (G, H, R)$ be either the triple

$$(\mathrm{Mlt}_\rho(Q), \mathrm{Inn}_\rho(Q), \{R_i; i \in Q\}),$$

or the triple

$$(\mathrm{Mlt}(Q), \mathrm{Inn}(Q), \{R_i; i \in Q\}).$$

Then G is a transitive permutation group on $\{1, \ldots, d\}$, $H = G_1$, and R is a right transversal to H in G, since for $g \in G$ there is a unique i such that $g \in HR_i$, namely $i = 1g$.

Now consider an arbitrary group G, H a subgroup of G, and R a right transversal to H in G containing 1_G. Then we can define a binary operation $\circ$ on R by letting

$$x \circ y = z \text{ if and only if } xy \in Hz.$$

We claim that $(R, \circ)$ is a loop if and only if R is a right transversal to every conjugate H^g in G. Indeed, given y, $z \in R$, the equation $x \circ y = z$ has a unique solution in R if and only if x is the unique element of $Hzy^{-1} \cap R$; and, given x, $z \in R$, the equation $x \circ y = z$ has a unique solution in R if and only if y is the unique element of $H^x(x^{-1}z) \cap R$. There is a neutral element in $(R, \circ)$ thanks to $1_G \in R$.

Moreover, if Q is a loop and $\mathcal{F}(Q) = (G, H, R)$, then the loop $(R, \circ)$ is isomorphic to Q, since $R_i \circ R_j = R_k$ if and only if $R_iR_j \in HR_k$, which happens if and only if $ij = 1R_iR_j = 1HR_k = k$.

To find all loops of order d, it therefore suffices to consider all transitive permutation groups G on $Q = \{1, \ldots, d\}$, $H = G_1$, and all right transversals $R = \{r_i; i \in Q\}$ to all $H^g \in G$, where we can assume without loss of generality that $ir_1 = 1r_i = i$ for every $i \in Q$. Note that we can then transfer the operation $\circ$ from R to the underlying set Q by letting $i \circ j = k$ if and only if $r_i \circ r_j = r_k$.

It is natural to consider another operation $*$ on Q by declaring the mappings r_i to be the right translations of $(Q, *)$, that is, by letting $i * j = ir_j$ for i, $j \in Q$. Lemma 2.2 shows that $(Q, \circ) = (Q, *)$.

LEMMA 2.1. *Let $R = \{r_i; i \in Q\}$ be a set of bijections of $Q = \{1, \ldots, d\}$ such that $ir_1 = 1r_i = i$ for every $i \in Q$. Then $(Q, *)$ is a loop with neutral element 1 if and only if $r_ir_j^{-1}$ is fixed point free for every $i \neq j \in Q$.*

Proof. Note that 1 is the neutral element of $(Q, *)$ since $i * 1 = ir_1 = i = 1r_i = 1 * i$ for every $i \in Q$. By definition, the right translation R_j by j in $(Q, *)$ coincides with r_j. Moreover, the following conditions are equivalent for i, j, $k \in Q$: $kr_ir_j^{-1} = k$, $kr_i = kr_j$, $k * i = k * j$.

If $(Q, *)$ is a loop, we deduce that $r_ir_j^{-1}$ is fixed point free whenever $i \neq j$. Conversely, if $r_ir_j^{-1}$ is fixed point free for every $i \neq j$, we see that every left translation L_k in $(Q, *)$ is one-to-one, hence onto. Since, by assumption, every right translation of $(Q, *)$ is a bijection, $(Q, *)$ is a loop. □

LEMMA 2.2. *Let G be a transitive permutation group on $Q = \{1, \dots, d\}$, $H = G_1$, and $R = \{r_i; i \in Q\} \subseteq G$ such that $ir_1 = 1r_i = i$ for every $i \in Q$. Then R is a transversal to every conjugate H^g in G if and only if $r_i r_j^{-1}$ is fixed point free for every $i \neq j \in Q$. If this condition is satisfied, the loops $(Q, \circ)$ and $(Q, *)$ coincide.*

Proof. Assume that R is a transversal to every conjugate H^g in G. Then $(Q, \circ)$ is a loop, where, recall, $i \circ j = k$ if and only if $r_i r_j \in Hr_k$. Moreover, $1r_i r_j = ir_j = 1Hr_{ir_j}$, so $r_i r_j \in Hr_{ir_j}$, $i \circ j = ir_j = i * j$, and $(Q, *) = (Q, \circ)$ coincide.

Conversely, assume that $r_i r_j^{-1}$ is fixed point free for every $i \neq j$. Then $(Q, *)$ is a loop with neutral element 1 by Lemma 2.1. Since R is a right transversal to H in G, $(Q, \circ)$ is defined. The equality $i \circ j = i * j$ then follows as above. □

Constructing all loops from suitable subsets R of right translations in transitive permutation groups is obviously prohibitive already for rather small values of d. But we can take advantage of the following results that greatly restrict the possible transitive groups G in general, and the subsets R in the case of automorphic loops.

3. *Simple loops and primitive groups*

Recall that a transitive permutation group on Q is *primitive* if it preserves no non-trivial partition of Q. The *degree* of a primitive group is the number of points it moves, that is, the cardinality of Q. Note that every 2-transitive group is primitive.

The following result is well known, with earliest reference likely [**1**, Theorem 8].

PROPOSITION 3.1 (Albert). *A loop Q is simple if and only if its multiplication group* $\mathrm{Mlt}(Q)$ *is primitive on Q.*

Proof. Assume that Q is not simple, and let S be a non-trivial normal subloop of Q. Then for every $x, y \in Q$ we have $xS = Sx$ since S is invariant under conjugations, $(yS)L_x = x(yS) = (xy)S$ since S in invariant under left inner mappings, and $(yS)R_x = (Sy)R_x = (Sy)x = S(yx) = (yx)S$ since S is invariant under right inner mappings. Thus $\mathrm{Mlt}(Q)$ preserves the non-trivial partition $\{yS; y \in Q\}$ of Q, so it is not primitive on Q.

Conversely, assume that $\mathrm{Mlt}(Q)$ is not primitive on Q, and let $\{B_1, \dots, B_m\}$ be a non-trivial partition of Q preserved by $\mathrm{Mlt}(Q)$. Without loss of generality, let $S = B_1$ be the block containing 1. With $x, y \in Q$, both SL_x and SR_x contain x, so $xS = Sx$, and, similarly, $x(yS) = (xy)S$ and $(Sx)y = S(xy)$. Hence S is a normal subloop of Q. If $|S| = 1$ then $|B_j| = 1$ for every j, as $\mathrm{Mlt}(Q)$ acts transitively on Q, a contradiction. □

Building upon the work of O'Nan and Scott, Aschbacher, Dixon and Mortimer, to name a few, Roney-Dougal classified all primite groups of degree less than 2500 [**30**]. (See [**30**, Section 1] for an extensive historical background concerning the classification.)

These groups are conveniently accessed in the GAP [**14**] library 'Primitive Permutation Groups'. The GAP command `NrPrimitiveGroups(`d`)` returns the number of primitive groups of degree d, and the ith primitive group of degree d is retrieved with the command `PrimitiveGroup(`d, i`)`.

The main reason why we were not able to expand the scope of Theorems 1.1 and 1.2 is the extent of the available libraries of primitive groups.

4. *Multiplication groups of automorphic loops*

It follows from the classification of finite simple groups that the only 4-transitive groups are the symmetric groups S_n for $n \geqslant 4$, the alternating groups A_n for $n \geqslant 6$, and the Mathieu

groups M_{11}, M_{12}, M_{23} and M_{24}. Corollary 4.3 below therefore does not disqualify many primitive groups from being multiplication groups of automorphic loops, but, importantly, it disqualifies the computationally most difficult symmetric and alternating groups.

REMARK 4.1. It appears that it is rare for a simple loop to have a multiplication group different from A_n and S_n. This statement could likely be made more precise by modifying Cameron's proof [7] of the following result: *the rows (viewed as permutations) of a randomly chosen latin square of order n generate either A_n or S_n with probability approaching* 1 *as n approaches infinity.*

LEMMA 4.2. *Let Q be a loop and H a subgroup of* $\mathrm{Aut}(Q)$. *Then for every i, $j \in Q$ the product ij belongs to a trivial orbit of the pointwise stabilizer $H_{i,j}$. In particular, H is not* 3*-transitive on $Q\backslash\{1\}$, except for the case $Q = C_2 \times C_2$ and $H = \mathrm{Aut}(Q) = S_3$.*

Proof. Assume that $ij = k$ and k is not in a trivial orbit of $H_{i,j}$. Then there is $h \in H$ such that $ih = i$, $jh = j$ and $kh \neq k$. Thus $ij = ih \cdot jh = (ij)h = kh \neq k$, a contradiction.

Assume that H is 3-transitive on $Q\backslash\{1\}$. If $|Q| > 4$, then the transitive $H_{i,j}$ has a non-trivial orbit. The only loops of order 4 are C_4 with $\mathrm{Aut}(C_4) = C_2$, and $C_2 \times C_2$ with $\mathrm{Aut}(C_2 \times C_2) = S_3$. □

COROLLARY 4.3. *Let Q be an automorphic loop. Then* $\mathrm{Inn}(Q)$ *is not* 3*-transitive on $Q\backslash\{1\}$ and* $\mathrm{Mlt}(Q)$ *is not* 4*-transitive on Q.*

Proof. Since $\mathrm{Inn}(Q) = \mathrm{Mlt}(Q)_1 \leqslant \mathrm{Aut}(Q)$, we are done by Lemma 4.2 as long as $Q \neq C_2 \times C_2$. But if $Q = C_2 \times C_2$ then $\mathrm{Inn}(Q) = 1$. □

The right translations of an automorphic loop are linked by the action of the inner mapping group.

LEMMA 4.4. *Let Q be a loop and h a permutation of Q. Then $h \in \mathrm{Aut}(Q)$ if and only if $R_i^h = R_{ih}$ for every $i \in Q$.*

Proof. The following conditions, all universally quantified for $j \in Q$, are equivalent for i and h: $R_i^h = R_{ih}$, $jh^{-1}R_ih = jR_{ih}$, $(jh^{-1} \cdot i)h = j(ih)$, $(ji)h = jh \cdot ih$. □

COROLLARY 4.5. *A loop Q is automorphic if and only if $R_i^h = R_{ih}$ for every $i \in Q$ and $h \in \mathrm{Inn}(Q)$.*

Here is a summary of results that will be used to explain the algorithm of Section 5.

PROPOSITION 4.6. *Let Q be a loop and $H \leqslant \mathrm{Aut}(Q)$. Then the following results hold.*

(i) *$R_i^h = R_{ih}$ for every $i \in Q$ and $h \in H$.*

(ii) *$|R_i^H| = |iH|$ for every $i \in Q$.*

(iii) *There exists $I \subseteq Q$ such that $\sum_{i\in I} |iH| = |Q|$ and such that $\{R_i; i \in Q\}$ is the disjoint union $\bigcup_{i\in I} R_i^H$.*

(iv) *R_i commutes with every element of the stabilizer H_i, for $i \in Q$.*

(v) *$R_iR_j^{-1}$ is fixed point free for every distinct i, $j \in Q$.*

Proof. Parts (i), (ii) and (iii) follow from Lemma 4.4. Let $h \in H_i$. Then for every $j \in Q$ we have $jhR_i = jh \cdot i = jh \cdot ih = (ji)h = jR_ih$, proving (iv). Part (v) follows from Lemma 2.1. □

5. *Loops with prescribed automorphisms*

Let G be a transitive permutation group on a finite set Q, and let $H = G_1$. The following algorithm efficiently searches for all loops $Q = (Q, *)$ (with fixed neutral element 1) such that $\mathrm{Mlt}_\rho(Q) \leqslant G$ and $H \leqslant \mathrm{Aut}(Q)$. The loops $(Q, *)$ will be constructed by means of the set $R = \{r_i; i \in Q\} \subseteq G$, where r_i will be the right translation by i in $(Q, *)$. As usual, we can assume without loss of generality that $ir_1 = 1r_i = i$ for every $i \in Q$. All references in the algorithm are to Proposition 4.6.

Algorithm 5.1.

Step 1. Set $r_1 = 1_G$. Find $I \subseteq Q$ such that the disjoint union $\bigcup_{i \in I} iH$ is equal to $Q \backslash \{1\}$.

Step 2. For $i \in I$, find $\mathcal{R}_i$, the set consisting of all candidates r_i for the right translation by i, as follows: by (iv), (v) and the fact that $r_1 = 1_G \in R$, r_i must be fixed point free, in the centralizer $C_G(H_i)$, and such that $1r_i = i$. If there is no such r_i, the algorithm stops with failure. Else it suffices to find one such r_i, and set $\mathcal{R}_i$ equal to the coset $(C_G(H_i))_1 r_i$, because $1s = i$ if and only if $1sr_i^{-1} = 1$.

Step 3. For $i \in I$, find $\mathbf{R}_i$, the set consisting of candidate orbits r_i^H with $r_i \in \mathcal{R}_i$, as follows: let $r_i \in \mathcal{R}_i$. If $|r_i^H| \neq |iH|$, discard r_i, by (ii). If there is $s \in r_i^H$ such that $s \neq r_i$ and sr_i^{-1} is not fixed point free, discard r_i, by (v). Else add r_i^H into $\mathbf{R}_i$.

Step 4. For i, $j \in I$, decide which pairs $r_i^H \in \mathbf{R}_i$, $r_j^H \in \mathbf{R}_j$ do not contradict (v): call two candidate orbits r_i^H, r_j^H with $i \neq j$ *compatible* if st^{-1} is fixed point free for every $s \in r_i^H$ and $t \in r_j^H$. Compatibility is a symmetric relation, so it suffices to consider orbits r_i^H, r_j^H with $i < j$. To decide if r_i^H, r_j^H with $i < j$ are compatible, it suffices to check that all permutations in $r_j^H r_i^{-1}$ (rather than in $r_j^H (r_i^H)^{-1}$) are fixed point free. Indeed, if $kr_i^{h_i} = kr_j^{h_j}$ for some $k \in Q$ and h_i, $h_j \in H$, then $(kh_i^{-1})r_i = (kh_i^{-1})r_j^{h_j h_i^{-1}}$.

Step 5. Put together pairwise compatible candidate orbits to form the set of loop translations $\{r_i; 1 < i \in Q\}$: this can be done elegantly with the use of graph algorithms in the GAP package GRAPE [**31**]. The compatibility relation from Step 4 corresponds to the edges of a graph $\mathcal{G}$ whose vertices are the candidate orbits r_i^H. Assign vertex weight $|r_i^H|$ to r_i^H, and return all complete subgraphs of $\mathcal{G}$ whose vertex weights add up to $|Q| - 1$.

Here is the GAP code for the algorithm (it can be downloaded from the web site of the last author at http://www.math.du.edu/~petr).

```
RightAutomorphicLoopsWithPrescribedAutomorphisms := function(g)
# returns all loops Q whose right multiplication group is a subgroup of g
# and Stabilizer(g, 1) is a subgroup of Aut(Q)
    local d, h, c, v, ls, x, i, j, k, orbs, orbit, new, graph, comp, cs;
    # Step 1
    d := NrMovedPoints(g);
    h := Stabilizer(g, 1);
    orbs := Set(Orbits(h, [2..d]), Set);
    # Steps 2 and 3
    ls := [];
    for orbit in orbs do
        c := Centralizer(g, Stabilizer(h, orbit[1]));
        v := RepresentativeAction(c, 1, orbit[1]);
        if v <> fail then
            v := RightCoset(Stabilizer(c, 1), v);
```

```
            v := Filtered(v, x -> NrMovedPoints(x) = d);
            new := [];
            for x in v do
                k := Orbit(h, x);
                if ForAll(k/k[1], y -> NrMovedPoints(y) in [0,d])
                    and Length(k) = Length(orbit)
                    then Add(new, k);
                fi;
            od;
            Add(ls, new);
        fi;
    od;
    ls := Concatenation(ls);
    # Step 4
    comp := List([1..Length(ls)], i -> []);
    for i in [1..Length(ls)] do
        for j in [1..i] do
            if ForAll(ls[i]/ls[j][1], p -> NrMovedPoints(p) = d) then
                comp[i][j] := true;
                comp[j][i] := true;
            else
                comp[i][j] := false;
                comp[j][i] := false;
            fi;
        od;
    od;
    # Step 5
    graph := Graph(Group(()), [1..Length(comp)], OnPoints,
        function(x, y) return comp[x][y]; end);
    cs := CompleteSubgraphsOfGivenSize(
            graph, d-1, 1, false, true, List(ls, Length));
    cs := List(cs, x -> VertexNames(graph){x});
    cs := List(cs, x -> Concatenation(ls{x}));
    cs := List(cs, x -> SortedList(Concatenation([()], x)));
    return cs;
end;
```

6. *The search for simple (right) automorphic loops*

Since the algorithm of Section 5 is delicate, we first present some comments and then give the results. We assume that the input of the algorithm is a permutation group G primitive on the set Q.

6.1. *Discussion of the algorithm*

The algorithm returns all loops $Q = (Q, *)$ *such that* $\mathrm{Mlt}_\rho(Q) \leqslant G$ *and* $G_1 = H \leqslant \mathrm{Aut}(Q)$. Indeed, the inclusion $\mathrm{Mlt}_\rho(Q) \leqslant G$ is obvious. Step 3 and Lemma 4.4 guarantee that $H \leqslant \mathrm{Aut}(Q)$, since for every $h \in H$ and $i \in Q$ we have $1r_i^h = 1h^{-1}r_i h = 1r_i h = ih$, hence $r_{ih} = r_i^h$. Steps 3, 4 and 5 guarantee that every $r_i r_j^{-1}$ with $i \neq j$ is fixed point free, so $(Q, *)$ is a loop by Lemma 2.1.

All returned loops are right automorphic. We have $\mathrm{Mlt}_\rho(Q) \leqslant G$, so $\mathrm{Inn}_\rho(Q) \leqslant G_1 \leqslant \mathrm{Aut}(Q)$.

Not all returned loops are necessarily simple. The condition $\mathrm{Mlt}_\rho(Q) \leqslant G$ does not guarantee that either $\mathrm{Mlt}_\rho(Q)$ or $\mathrm{Mlt}(Q)$ is primitive. If it happens that $\mathrm{Mlt}_\rho(Q) = G$ then both $\mathrm{Mlt}_\rho(Q)$ and $\mathrm{Mlt}(Q)$ are primitive, hence Q is simple.

Not all finite simple right automorphic loops are found. Let Q be a simple right automorphic loop and $G = \mathrm{Mlt}(Q)$. Then the algorithm with input G returns Q if and only if $\mathrm{Inn}(Q) = G_1 \leqslant \mathrm{Aut}(Q)$, that is, if and only if Q is automorphic. Thus, when Q is right automorphic but not automorphic, it will not be found with input G, but it *could* be found with a different primitive

group as the input. Furthermore, if Q is a simple right automorphic that is not automorphic and if $\mathrm{Mlt}_\rho(Q)$ is imprimitive (such loops exist), then Q will not be found by the algorithm applied to any primite group.

We can skip 4-transitive groups. If G is 4-transitive then $H = G_1$ is 3-transitive and no non-associative loop Q with $H \leqslant \mathrm{Aut}(Q)$ exists, by Lemma 4.2.

While searching for simple automorphic loops, it suffices to consider groups of even degree. By a result of [**21**], a non-associative finite simple automorphic loop is of even order.

While searching for simple commutative automorphic loops, it suffices to consider groups of degree a power of two. By [**19**, Proposition 6.1, Theorem 6.2], a non-associative finite simple commutative automorphic loop is of order a power of two.

While searching for simple automorphic loops, we can skip solvable groups. Vesanen proved [**34**] that any loop with solvable multiplication group is itself solvable. Hence if Q is a non-associative simple automorphic loop then $G = \mathrm{Mlt}(Q)$ is not solvable, and Q will be found by the algorithm with input G. (Of course, Q could also be found by the algorithm with some solvable group as the input.)

While systematically searching for simple automorphic loops, it is not necessary to check that all inner mappings are automorphisms. If $\mathrm{Mlt}(Q) = G$ then $\mathrm{Inn}(Q) \leqslant \mathrm{Aut}(Q)$ and Q is a simple automorphic loop. If $\mathrm{Mlt}(Q) \neq G$ then we can ignore Q because either $\mathrm{Mlt}(Q)$ is not primitive (and Q is not simple), or $\mathrm{Mlt}(Q)$ is primitive, in which case Q will be found again by the algorithm with input $\mathrm{Mlt}(Q)$.

6.2. *Results*

Simple right automorphic loops. We found all non-associative simple right automorphic loops Q up to isomorphism with the following properties: $|Q| < 504$, there exists a primitive group G of degree $|Q|$ such that $\mathrm{Mlt}_\rho(Q) \leqslant G$ and $G_1 \leqslant \mathrm{Aut}(Q)$.

The following table summarizes the results.

Order	15	27	60	64	81	125	168	243	256	343	360
Found loops	1	1	5	1	2	6	11	60	2	28	17

To do this, it suffices to (i) apply Algorithm 5.1 to all primitive groups G of degree less than 504 that are not 4-transitive, (ii) to filter the resulting loops for simplicity, (iii) to filter all remaining loops up to isomorphism.

Concerning (ii): in most cases we quickly observe $\mathrm{Mlt}_\rho(Q) = G$, which means that G is simple. In the few remaining cases when $\mathrm{Mlt}_\rho(Q) < G$ we must calculate $\mathrm{Mlt}(Q)$ and check for primitivity.

Concerning (iii): we used the isomorphism filter for loops built into the Loops [**26**] package of GAP. The isomorphism filtering takes up most of the running time of the search, and it is one of the reasons why we decided to stop at order 504. The other reason is that the search does not find all non-associative simple right automorphic loops, as we have already pointed out in the Introduction, so it is not clear how useful the results are for large orders.

The running time of the search was about 30 minutes on a 2 GHz processor PC.

Simple automorphic loops. By running the algorithm on all primitive groups of even degree less than 2500 that are neither 4-transitive nor solvable, we established Theorem 1.2, a somewhat surprising result.

The running time of the search was about 20 minutes.

Simple commutative automorphic loops. Theorem 1.1 now follows, too. But it is possible to obtain it faster, by running the algorithm on all primitive groups of degree a power of two and less than 2^{12} that are neither 4-transitive nor solvable.

The running time of the search was about 2 minutes.

7. *Right automorphic loops and conjugations*

As discussed in Section 6, it is never necessary to check that inner mappings are automorphisms while systematically searching for simple automorphic loops by Algorithm 5.1. But it is necessary to run the check if we wish to find all automorphic loops with $\mathrm{Mlt}_\rho(Q) \leqslant G$ and $G_1 \leqslant \mathrm{Aut}(Q)$ for a fixed primitive group G. The following result, which is of independent interest, shows that it is not necessary to check the left inner mappings.

THEOREM 7.1. *Let Q be a right automorphic loop. Then Q is automorphic if and only if all conjugations T_x, $x \in Q$, are automorphisms of Q.*

The rest of this section forms the proof of Theorem 7.1.

Recall that a loop is *flexible* if it satisfies the identity $xy \cdot x = x \cdot yx$, that is, $L_x R_x = R_x L_x$ for all x. Flexible loops have two-sided inverses. Indeed, if x^λ and x^ρ denote the left and right inverses of x, respectively, then $x = 1 \cdot x = xx^\rho \cdot x = x \cdot x^\rho x$ implies $x^\rho x = 1$, and since $x^\lambda x = 1$, we have $x^\rho = x^\lambda = x^{-1}$.

LEMMA 7.2. *Let Q be a loop in which every conjugation T_x, $x \in Q$, is an automorphism. Then Q is flexible.*

Proof. For $x, y \in Q$ we have $yL_xT_x = (xy)T_x = xT_x \cdot yT_x = x \cdot yT_x = yT_xL_x$ because T_x is an automorphism. Thus $L_xT_x = T_xL_x$ and $L_xR_x = L_xT_xL_x = T_xL_xL_x = R_xL_x$. □

LEMMA 7.3. *Let Q be a flexible, right automorphic loop. Then for all $x \in Q$,*

$$R_{x,x^{-1}} = R_{x^{-1},x}, \tag{7.1}$$

$$L_xR_{x^{-1}} = R_{x^{-1}}L_x, \tag{7.2}$$

$$L_{x^{-1}}R_x^{-1} = R_x^{-1}L_{x^{-1}}. \tag{7.3}$$

Proof. Note that $x^{-1}R_{x,x^{-1}} = x^{-1}$, thus

$$yR_{x^{-1}}R_{x,x^{-1}} = (yx^{-1})R_{x,x^{-1}} = yR_{x,x^{-1}} \cdot x^{-1}R_{x,x^{-1}} = yR_{x,x^{-1}} \cdot x^{-1} = yR_{x,x^{-1}}R_{x^{-1}},$$

or

$$R_{x^{-1}}R_{x,x^{-1}} = R_{x,x^{-1}}R_{x^{-1}}.$$

Then

$$R_{x^{-1},x}R_{x^{-1}} = R_{x^{-1}}R_xR_{x^{-1}} = R_{x^{-1}}R_{x,x^{-1}} = R_{x,x^{-1}}R_{x^{-1}},$$

which yields (7.1).

Similarly, by (7.1), we have $xR_{x,x^{-1}} = xR_{x^{-1},x} = x$, therefore

$$yL_xR_{x,x^{-1}} = (xy)R_{x,x^{-1}} = xR_{x,x^{-1}} \cdot yR_{x,x^{-1}} = x \cdot yR_{x,x^{-1}} = yR_{x,x^{-1}}L_x,$$

or

$$L_xR_{x,x^{-1}} = R_{x,x^{-1}}L_x.$$

Then, by flexibility,

$$R_xL_xR_{x^{-1}} = L_xR_xR_{x^{-1}} = L_xR_{x,x^{-1}} = R_{x,x^{-1}}L_x = R_xR_{x^{-1}}L_x,$$

and (7.2) follows.

Finally, (7.3) follows from (7.2) upon replacing x with x^{-1} and rearranging. □

A loop with two-sided inverses is said to have the *antiautomorphic inverse property* if it satisfies the identity $(xy)^{-1} = y^{-1}x^{-1}$. If we use J to denote the inversion permutation $x \mapsto x^{-1}$, then the antiautomorphic inverse property is equivalent to $R_y^J = L_{y^{-1}}$ for all y, or to $L_y^J = R_{y^{-1}}$ for all y.

PROPOSITION 7.4. *A flexible, right automorphic loop has the antiautomorphic inverse property.*

Proof. By (7.3), $(x^{-1}y^{-1})R_x^{-1} = y^{-1}R_x^{-1}L_{x^{-1}}$. Let us apply $R_{x,y}$ to both sides. On the left side we get $(x^{-1}y^{-1})R_x^{-1}R_{x,y} = (x^{-1}y^{-1})R_yR_{xy}^{-1}$. On the right side we get

$$\begin{aligned} y^{-1}R_x^{-1}L_x^{-1}R_{x,y} &= (x^{-1}\cdot y^{-1}R_x^{-1})R_{x,y} = x^{-1}R_{x,y}\cdot y^{-1}R_x^{-1}R_{x,y} \\ &= yR_{xy}^{-1}\cdot(xy)^{-1} = yR_{xy}^{-1}R_{(xy)^{-1}}. \end{aligned}$$

Hence $(x^{-1}y^{-1})R_yR_{xy}^{-1} = yR_{xy}^{-1}R_{(xy)^{-1}}$, so

$$(x^{-1}y^{-1})R_y = yR_{xy}^{-1}R_{(xy)^{-1}}R_{xy} = yR_{xy}^{-1}R_{xy}R_{(xy)^{-1}} = yR_{(xy)^{-1}} = xR_yJL_y,$$

where we have used (7.1) in the second equality. Now,

$$(x^{-1}y^{-1})R_y = xJR_{y^{-1},y} = xR_{y^{-1},y}J = xR_{y,y^{-1}}J = xR_yR_{y^{-1}}J,$$

using the fact that $R_{y^{-1},y}$ is an automorphism in the second equality, and (7.1) in the third.

Thus we have $R_yJL_y = R_yR_{y^{-1}}J$, or $L_y^J = R_{y^{-1}}$, which is the antiautomorphic inverse property. □

Combining Lemma 7.2 and Proposition 7.4 yields the following theorem.

THEOREM 7.5. *Every automorphic loop has the antiautomorphic inverse property.*

We can now finish the proof of Theorem 7.1 as follows: the necessity of the condition is obvious, so let us prove sufficiency. By Lemma 7.2, Q is flexible. By Proposition 7.4, Q has the antiautomorphic inverse property. For each x, $y \in Q$, $R_{x,y}^J = JR_{x,y}J = R_{x,y}$, since $R_{x,y}$ is an automorphism. Hence

$$\begin{aligned} R_{x,y} = R_{x,y}^J &= R_x^JR_y^J(R_{xy}^{-1})^J = R_x^JR_y^J(R_{xy}^J)^{-1} = L_{x^{-1}}L_{y^{-1}}L_{(xy)^{-1}}^{-1} \\ &= L_{x^{-1}}L_{y^{-1}}L_{y^{-1}x^{-1}}^{-1} = L_{x^{-1},y^{-1}} \end{aligned}$$

by the antiautomorphic inverse property. This implies that every inner mapping of Q is an automorphism, and we are through.

8. *Additional theoretical results*

We have by now proved the theorems from the Introduction by a computer search based on Algorithm 5.1 and several theoretical results. However, as we are going to explain next, some degrees $d = 2^m$ can be eliminated without such a search, by taking advantage of certain results about primitive groups of affine type and permutation groups realizable as multiplication groups of loops. We will still need some computer calculations, but only of rather routine character, such as determining the size of the smallest non-trivial conjugacy class of a given group.

8.1. *Groups that are (not) multiplication groups of loops*

The question of which (transitive permutation) groups are multiplication groups of loops has been studied but remains largely unanswered. Although we will only need some of the known results below, we include them for the sake of completeness. All groups are assumed to be in their natural permutation representation.

PROPOSITION 8.1. *The following groups are multiplication groups of loops:*
(i) S_n *for* $n \geqslant 2$ [9];
(ii) A_n *for* $n \geqslant 6$ [12];
(iii) M_{12} [8];
(iv) M_{24} [25].
If $n \geqslant 3$ *and* $q^n > 8$ *then there is a loop* Q *with* $\mathrm{PSL}(n,q) \leqslant \mathrm{Mlt}(Q) \leqslant \mathrm{PGL}(n,q)$ [25].

PROPOSITION 8.2. *The following groups are not multiplication groups of loops:*
(i) $\mathrm{PSL}(2,q)$ *for* $q \geqslant 3$ [32];
(ii) M_{11}, M_{23} [11];
(iii) $\mathrm{PSL}(2n,q)$ *with* $q \geqslant 5$, $\mathrm{PU}(n,q^2)$ *with* $n \geqslant 6$, $\mathrm{PO}(n,q)$ *with* $n \geqslant 7$ *odd*, $\mathrm{PO}^{\varepsilon}(n,q)$ *with* $n \geqslant 7-\varepsilon$ *even* [33].
Furthermore, if every $1 \neq \alpha \in \mathrm{Mlt}(Q)$ *fixes at most two points then* Q *is an abelian group* [10].
If $\mathrm{Mlt}(Q) \leqslant \mathrm{P\Gamma L}(2,q)$ *and* $q \geqslant 5$ *then* Q *is an abelian group* [11].

8.2. *Primitive groups of affine type*

Recall that the *socle* $\mathrm{Soc}(G)$ of a group G is the subgroup (necessarily normal) of G generated by all minimal normal subgroups of G. Also recall that a permutation group G on X is *regular* if it is sharply transitive, that is, for every $i, j \in X$ there is unique $g \in G$ such that $ig = j$.

Of great importance in the classification of primitive groups is the O'Nan–Scott theorem (see, for instance [30]). We will only need the part of the O'Nan–Scott theorem concerned with abelian socle.

THEOREM 8.3. *Let* G *be a primitive group of degree* d*, and let* $U = \mathrm{Soc}(G)$*. Then* U *is abelian if and only if* U *is a regular, elementary abelian* p*-group of order* $d = p^n$ *and* G *is isomorphic to a subgroup of the affine linear group* $\mathrm{AGL}(n,p)$.

Primitive groups with abelian socle are therefore called of *affine type*.

Let Q be a simple commutative automorphic loop, and let $R = \{r_i; i \in Q\}$ be the right translations of Q, with $ir_1 = 1r_i = i$ for $i \in Q$. Assume that $G = \mathrm{Mlt}(Q)$ is a primitive group of affine type of degree d and $H = G_1$. Let also $U = \mathrm{Soc}(G)$. Since U is a normal regular subgroup of G, we have $|U| = |Q| = d$, and we can write $U = \{u_i; i \in Q\}$ with some u_i satisfying $1u_i = i$. Note that U is a right transversal to H in G. There are thus uniquely determined $h_i \in H$ such that $r_i = h_i u_i$ for $i \in Q$. We will call this situation the *affine setup*.

Note that in the affine setup we can define an isomorphic copy of the loop Q on U by letting $u_i \bullet u_j = u_i^{h_j} u_j$, since $r_i r_j = h_i u_i h_j u_j = h_i h_j u_i^{h_j} u_j \in H r_{ij} = H h_{ij} u_{ij} = H u_{ij}$.

LEMMA 8.4. *In the affine setup,* $\langle h_i; i \in Q \rangle = H$.

Proof. Note that $r_i r_j r_{ij}^{-1} r_{ij} = r_i r_j = h_i h_j u_i^{h_j} u_j = h_i h_j u_{ij} = h_i h_j h_{ij}^{-1} r_{ij}$, and thus $r_i r_j r_{ij}^{-1} = h_i h_j h_{ij}^{-1}$. Since Q is commutative, we are done by $H = \mathrm{Inn}(Q) = \mathrm{Inn}_{\rho}(Q) = \langle r_i r_j r_{ij}^{-1}; i, j \in Q \rangle = \langle h_i h_j h_{ij}^{-1}; i, j \in Q \rangle \leqslant \langle h_i; i \in Q \rangle \leqslant H$. □

We will need the following result of Niemenmaa and Kepka [29].

THEOREM 8.5 (Niemenmaa and Kepka). *Let* Q *be a finite loop such that* $\mathrm{Inn}(Q)$ *is abelian. Then* Q *is nilpotent.*

REMARK 8.6. Building upon the work of Mazur [23], Niemenmaa obtained a more general result in [27]: *let* Q *be a finite loop such that* $\mathrm{Inn}(Q)$ *is nilpotent. Then* Q *is nilpotent.*

PROPOSITION 8.7. *In the affine setup, if $h_i \in Z(H)$ for every $i \in Q$, then Q is a cyclic group of prime order.*

Proof. Assume that $h_i \in Z(H)$ for every $i \in Q$. By Lemma 8.4, $\mathrm{Inn}(Q) = H = Z(H)$ is an abelian group. By Theorem 8.5, Q is nilpotent. Since Q is simple, it follows that $Q = Z(Q)$ is a simple abelian group, necessarily a cyclic group of prime order. □

PROPOSITION 8.8. *In the affine setup, let γ be the size of a largest orbit of H on Q. If Q is not associative, then H contains a conjugacy class C of size $1 < |C| \leqslant \gamma$.*

Proof. If every conjugacy class h_i^H is trivial then Q is a group by Proposition 8.7. Thus we can assume that there is $C = h_i^H$ such that $|C| > 1$. By Lemma 4.4, $h_i^m u_i^m = r_i^m = r_{im} = h_{im} u_{im}$ for every $m \in H$. Since U is normal in G, $u_i^m = u_j$ for some j, in fact, $j = 1u_j = 1u_i^m = 1m^{-1}u_i m = 1u_i m = im$. Thus $u_i^m = u_{im}$, and $h_i^m = h_{im}$ follows. Then $C = h_i^H = \{h_{im}; m \in H\}$, and thus $|C|$ cannot exceed the size of the H-orbit of i on Q. In particular, $|C| \leqslant \gamma$. □

8.3. *Simple commutative automorphic loops of orders* 32 *and* 128

To illustrate the theoretical results, we show, without the search of Section 5, that there are no non-associative simple commutative automorphic loops of orders 32 and 128.

Order 32. The groups A_{32} and S_{32} are 4-transitive, and can be eliminated by Lemma 4.2. The groups $\mathrm{AGL}(1, 32)$ and $\mathrm{A\Gamma L}(1, 32)$ are solvable, eliminated by [**34**]. The groups $\mathrm{PSL}(2, 31)$ and $\mathrm{PGL}(2, 31)$ are eliminated by Proposition 8.2. The group $\mathrm{ASL}(5, 2)$ has no non-trivial conjugacy class of size less than 32, so it is eliminated by Proposition 8.8. There are no other primitive groups of degree 32.

Order 128. The groups A_{128}, S_{128} are 4-transitive, and the groups $\mathrm{AGL}(1, 128)$, $\mathrm{A\Gamma L}(1, 128)$ are solvable. The groups $\mathrm{PSL}(2, 127)$, $\mathrm{PGL}(2, 127)$ are eliminated by Proposition 8.2. The group $\mathrm{AGL}(2, 7)$ has no non-trivial conjugacy class of size less than 128, so it is eliminated by Proposition 8.8. There are no other primitive groups of degree 128.

9. *Reformulation of the main problem to group theory*

We conclude this paper by restating Problem 1.3 entirely within group theory. We claim that Problem 1.3 is equivalent to the following.

PROBLEM 9.1. Is there a set Q containing 1, a permutation group G on Q, and a subset $R \subseteq G$ containing 1_G such that the following conditions hold?

(a) G is primitive on Q and $|Q| = 2^n > 2$.
(b) R is a right transversal to $H = G_1$ in G.
(c) $G = \langle R \rangle$.
(d) $[R^{-1}, R^{-1}] \leqslant H$.
(e) $R^h = R$ for every $h \in H$.

Indeed, assume that all conditions of Problem 9.1 are satisfied. By (b), we can assume that $R = \{r_i; i \in Q\}$, where $1r_i = ir_1 = i$ for every $i \in Q$. To show that the groupoid $(Q, *)$ defined by $i * j = ir_j$ is a loop, we use the following result, which can be deduced from [**28**, Lemmas 2.1 and 2.2].

LEMMA 9.2. *Let H be a subgroup of G and let A, B be right transversals to H such that $[A^{-1}, B^{-1}] \leqslant H$. Then both A and B are right transversals to every conjugate of H in G.*

Proof. Fix $x \in G$. Then $x = hb$ for unique $h \in H$, $b \in B$. Let $y \in G$. Then $yb^{-1} = ka$ for unique $k \in H$, $a \in A$. Then $y = kab = k[a^{-1}, b^{-1}]ba = k[a^{-1}, b^{-1}]h^{-1}xa \in Hxa$, so $G = \bigcup_{a \in A} Hxa$. Suppose that $Hxa \cap Hxc \neq \emptyset$ for some a, $c \in A$. Then $xac^{-1}x^{-1} \in H$, and $ac^{-1} = [a^{-1}, b^{-1}]h^{-1}hbac^{-1}b^{-1}h^{-1}h[b^{-1}, c^{-1}] = [a^{-1}, b^{-1}]h^{-1}(xac^{-1}x^{-1})h[b^{-1}, c^{-1}] \in H$, so $a = c$. This means that xA is a right transversal to H. Then for a given $g \in G$ there are unique $h \in H$, $a \in A$ such that $xg = hxa$, $g = h^x a$. Hence A is a right transversal to H^x. Similarly for B. □

By Lemma 9.2, (b) and (d), R is a right transversal to every conjugate of H in G. By Lemma 2.2, $(Q, *)$ is a loop. Since $\mathrm{Mlt}_\rho(Q) = \langle R \rangle = G$ by (c) and G is primitive by (a), $\mathrm{Mlt}(Q)$ is primitive on Q and hence Q is simple by Proposition 3.1. By (d), $1[r_i^{-1}, r_j^{-1}] = 1r_i r_j r_i^{-1} r_j^{-1} = 1$ for every i, j, so Q is commutative, $\mathrm{Mlt}(Q) = \mathrm{Mlt}_\rho(Q) = G$, and $\mathrm{Inn}(Q) = G_1 = H$. By (e), for every $i \in Q$ and every $h \in \mathrm{Inn}(Q) = H$ there is $j \in Q$ such that $r_i^h = r_j$. In this situation we have $1r_i^h = 1r_j$, $ih = j$, and so $r_i^h = r_{ih}$. By Corollary 4.5, Q is automorphic. Since $|Q| = 2^n > 2$ by (a), Q is not associative.

Conversely, if Q is a non-associative finite simple commutative automorphic loop, then we can take $G = \mathrm{Mlt}(Q)$, $R = \{R_i; i \in Q\}$, $H = G_1 = \mathrm{Inn}(Q)$, and observe (a) by Proposition 3.1 and [**19**, Proposition 6.1 and Theorem 6.2], (b) by Section 2, (d) because Q is commutative, (c) since $G = \mathrm{Mlt}(Q) = \mathrm{Mlt}_\rho(Q) = \langle R \rangle$, and (e) by Lemma 4.4.

While attempting to answer Problem 9.1, it will be useful to consider non-trivial consequences of (a)–(e). For instance, the following result holds if and only if the loop Q has exponent two, which must be true by [**19**].

(f) $\{r^2; r \in R\} \subseteq H$.

We are therefore interested in structural descriptions of primitive permutation groups of degree 2^n. The following result of Guralnick and Saxl is from [**17**].

THEOREM 9.3 (Guralnick and Saxl). *Let G be a primitive permutation group of degree 2^n. Then either G is of affine type, or G has a unique minimal normal subgroup $N = S \times \ldots \times S = S^t$, $t \geqslant 1$, S is a non-abelian simple group, and one of the following holds.*

(i) *$S = A_m$, $m = 2^e \geqslant 8$, $n = te$, and the point stabilizer in N is $N_1 = A_{m-1} \times \ldots \times A_{m-1}$.*

(ii) *$S = \mathrm{PSL}(d, q)$, $2^e = (q^d - 1)/(q - 1) \geqslant 8$, $d \geqslant 2$ is even, q is odd, $m = te$, and the point stabilizer in N is the direct product of maximal parabolic subgroups stabilizing either a 1-space or hyperplane in each copy.*

Acknowledgements. We thank Robert Guralnick for useful comments and for bringing Theorem 9.3 to our attention. We thank the anonymous referee who suggested several improvements to the presentation of the paper.

References

1. A. A. ALBERT, 'Quasigroups I', *Trans. Amer. Math. Soc.* 54 (1943) 507–519.
2. M. ASCHBACHER, 'On Bol loops of exponent 2', *J. Algebra* 288 (2005) no. 1, 99–136.
3. R. BAER, 'Nets and groups', *Trans. Amer. Math. Soc.* 47 (1939) 110–141.
4. B. BAUMEISTER and A. STEIN, 'Self-invariant 1-factorizations of complete graphs and finite Bol loops of exponent 2', *Beiträge Algebra Geom.* 51 (2010) no. 1, 117–135.
5. R. H. BRUCK, *A survey of binary systems*, Ergebnisse der Mathematik und ihrer Grenzgebiete 20 (Springer, Berlin, 1971) third printing, corrected.
6. R. H. BRUCK and L. J. PAIGE, 'Loops whose inner mappings are automorphisms', *Ann. of Math.* (2) 63 (1956) 308–323.
7. P. J. CAMERON, 'Almost all quasigroups have rank 2', *Discrete Math.* 106/107 (1992) 111–115.
8. J. H. CONWAY, 'The Golay codes and Mathieu groups', *Sphere packings, lattices and groups* (eds J. H. Conway and N. J. A. Sloane; Springer, Berlin–New York, 1988) Chapter 11.
9. A. DRÁPAL, Latin squares and groups, MS Thesis, Charles University, Prague, 1979.

10. A. Drápal, 'Multiplication groups of finite loops that fix at most two points', *J. Algebra* 235 (2001) 154–175.
11. A. Drápal, 'Multiplication groups of loops and projective semilinear transformations in dimension two', *J. Algebra* 251 (2002) 256–278.
12. A. Drápal and T. Kepka, 'Alternating groups and latin squares', *European J. Combin.* 10 (1989) 175–180.
13. M. Funk and P. T. Nagy, 'On collineation groups generated by Bol reflections', *J. Geom.* 48 (1993) no. 1–2, 63–78.
14. The GAP group, GAP—groups, algorithms, and programming, version 4.4.12, 2008, available at http://www.gap-system.org.
15. E. G. Goodaire and D. A. Robinson, 'A class of loops which are isomorphic to all loop isotopes', *Canad. J. Math.* 34 (1982) 662–672.
16. E. G. Goodaire and D. A. Robinson, 'Semi-direct products and Bol loop', *Demonstratio Math.* 27 (1994) no. 3–4, 573–588.
17. R. M. Guralnick and J. Saxl, 'Monodromy groups of polynomials', *Groups of Lie type and their geometries (Como, 1993)*, London Mathematical Society Lecture Note Series 207 (Cambridge University Press, Cambridge, 1995) 125–150.
18. P. Jedlička, M. K. Kinyon and P. Vojtěchovský, 'Constructions of commutative automorphic loops', *Comm. Algebra* 38 (2010) no. 9, 3243–3267.
19. P. Jedlička, M. K. . Kinyon and P. Vojtěchovský, 'The structure of commutative automorphic loops', *Trans. Amer. Math. Soc.* 363 (2011) 365–384.
20. H. Kiechle, *Theory of K-loops*, Lecture Notes in Mathematics 1778 (Springer, Berlin, 2002).
21. M. K. Kinyon, K. Kunen, J. D. Phillips and P. Vojtěchovský, 'The structure of automorphic loops', Preprint.
22. A. Kreuzer, 'Inner mappings of Bruck loops', *Math. Proc. Cambridge Philos. Soc.* 123 (1998) no. 1, 53–57.
23. M. Mazur, 'Connected transversals to nilpotent groups', *J. Group Theory* 2 (2007) 195–203.
24. G. P. Nagy, 'A class of finite simple Bol loops of exponent 2', *Trans. Amer. Math. Soc.* 361 (2009) no. 10, 5331–5343.
25. G. P. Nagy, 'On the multiplication groups of semifields', *European J. Combin.* 31 (2010) no. 1, 18–24.
26. G. P. Nagy and P. Vojtěchovský, 'Loops: computing with quasigroups and loops in GAP, version 2.1.0', available at http://www.math.du.edu/loops.
27. M. Niemenmaa, 'Finite loops with nilpotent inner mapping groups are centrally nilpotent', *Bull. Aust. Math. Soc.* 79 (2009) 109–114.
28. M. Niemenmaa and T. Kepka, 'On multiplication groups of loops', *J. Algebra* 135 (1990) no. 1, 112–122.
29. M. Niemenmaa and T. Kepka, 'On connected transversals to abelian subgroups', *Bull. Aust. Math. Soc.* 49 (1994) no. 1, 121–128.
30. C. M. Roney-Dougal, 'The primitive permutation groups of degree less than 2500', *J. Algebra* 292 (2005) no. 1, 154–183.
31. L. H. Soicher, 'GRAPE, Graph algorithms using permutation groups, version 4.3', package for GAP, available at http://www.maths.qmul.ac.UK/∼leonard/grape/.
32. A. Vesanen, 'The group PSL$(2, q)$ is not the multiplication group of a loop', *Comm. Algebra* 22 (1994) 1177–1195.
33. A. Vesanen, 'Finite classical groups and multiplication groups of loops', *Math. Proc. Cambridge Philos. Soc.* 117 (1995) 425–429.
34. A. Vesanen, 'Solvable groups and loops', *J. Algebra* 180 (1996) no. 3, 862–876.

Kenneth W. Johnson
Penn State Abington
1600 Woodland Rd, Abington
PA 19001
USA

kwj1@psu.edu

Michael K. Kinyon
Department of Mathematics
University of Denver
2360 S Gaylord St, Denver
Colorado 80112
USA

mkinyon@math.du.edu

Gábor P. Nagy
Bolyai Institute
University of Szeged
Aradi vértanúk tere 1
H-6720 Szeged
Hungary

nagyg@math.u-szeged.hu

Petr Vojtěchovský
Department of Mathematics
University of Denver
2360 S Gaylord St, Denver
Colorado 80112
USA

petr@math.du.edu