IJMAO

International Journal of Mathematical Analysis and Optimization: Theory and Applications
Vol. 2019, No. 1, pp. 426 - 432

Holomorph of self-distributive quasigroup with key laws

S. O. Ogunrinade[1*], S. O. Ajala [2] J. O. Olaleru [3] And T.G. Jaiyéọlá [4]

1 *, Department of Mathematics, Federal College of Education, Abeokuta, Ogun State, Nigeria.
2, 3, Department of Mathematics, Faculty of Science, University of Lagos, Lagos, Nigeria.
4, Department of Mathematics, Obafemi Awolowo University, Ile-Ife, Nigeria.
Corresponding Author's email: dayotopson@gmail.com

Article Info
Received:16 December 2018 Revised: 26 January 2019
Accepted: 08 January 2019 Available online: 23 April 2019

Abstract

Holomorph theory has received some considerations in the past. The holomorph of an algebraic structure is a semi-direct product of it and a set of maps on it. In this paper, the study of the holomorphy of self-distributive quasigroup with key laws were carried out. Given a quasigroup $(Q,\cdot)$ a subsemigroup $E(Q,\cdot) = E(Q)$ of the endomorphism semigroup of Q with holomorph $H(Q) = E(Q) \times Q$. It was shown that $H(Q)$ is a left (right) distributive groupoid if and only if $E(Q,\cdot)$ is a left (right) distributive quasigroup and the generalized left (right) distributive law in $(Q,\cdot)$ hold. Also, it was shown that $H(Q)$ obeys the left (right) key law if and only if $E(Q,\cdot)$ obeys the left (right) key law and the generalized left (right) key law in $(Q,\cdot)$ hold. Therefore, $H(Q)$ is a distributive groupoid if and only if $E(Q,\cdot)$ is distributive quasigroup and the generalized distributive law in $(Q,\cdot)$ hold. Also, $H(Q)$ obeys the key laws if and only if $E(Q,\cdot)$ obeys key laws and the generalized key laws in $(Q,\cdot)$ hold. The results on the holomorph of left and right key laws were shown to be applicable to symmetric cryptography (secret key cryptosystem).

Keywords: Distributive quasigroup, Left-right sided quasigroup, Holomorph, cryptography.
MSC2010: Primary 20N02, 20N05, Secondary 94A60

1 Introduction

Let $(Q,\cdot)$ be a groupoid. A groupoid $(Q,\cdot)$ in which for each $a \in Q$ the mappings $L_a : Q \longrightarrow Q$ defined as $L_a x = a \cdot x$ and $R_a : Q \longrightarrow Q$, defined as $R_a x = x \cdot a$ are bijective is called a quasigroup. A quasigroup which is left distributive and also satisfies the left key law (LKL) is called left-sided quasigroup (LSQ) and a quasigroup which is right distributive and also satisfies the right key law (RKL) is called right sided quasigroup (RSQ).

Lemma 1.1. (Bruck, 1944)
Let $A(Q,\cdot)$ be a group of automorphisms of a quasigroup $(Q,\cdot)$. Let $H = A(Q) \times Q$ and for $(\alpha, x), (\beta, y) \in H$ content...

IJMAO

International Journal of Mathematical Analysis and Optimization: Theory and Applications
Vol. 2019, No. 1, pp. 426 - 432

define

$$(\alpha, x) \circ (\beta, y) = (\alpha\beta, x\beta \cdot y)$$

then $(H, \circ)$ is a quasigroup.

Remark 1.1. If $A(Q)$ is a group of automorphisms of a quasigroup $(Q, \cdot)$, then the quasigroup $(H, \circ)$, constructed above, is called the $A(Q)$-holomorph of $(Q, \cdot)$.

Distributive quasigroup and holomorph of a given quasigroup have been studied by different authors [1-5]. The holomorphs of quasigroups and loops have been considered in [3,6-7,8-12]. For more on quasigroups and loops in general, readers can consult [4] and [13].

Definition 1.1. *A quasigroup $(Q, \cdot)$ is left-sided if $x \cdot yz = xy \cdot xz$ and $x \cdot xy = y$ for all $x, y, z \in Q$. That is, a quasigroup $(Q, \cdot)$ is left-sided if $(Q, \cdot)$ is left distributive and satisfies the left key law (LKL).*

Definition 1.2. *A quasigroup $(Q, \cdot)$ is right-sided if $xy \cdot z = xz \cdot yz$ and $xy \cdot y = x$ for all $x, y, z \in Q$. That is, a quasigroup $(Q, \cdot)$ is right-sided if $(Q, \cdot)$ is right distributive and satisfies the right key law (RKL).*

Definition 1.3. *A quasigroup $(Q, \cdot)$ is left-right sided if it is distributive and satisfy the left and the right key laws.*

Robinson [2] introduced right-sided quasigroup and showed that right-sided quasigroup coextensive with Bruck loops. Bruck loop is a special type of Bol loop and a Bol loop $(Q, \cdot)$ is a Bruck loop if

1. $x \to x^2$ is a permutation of Q and
2. $xy^2 \cdot x = (yx)^2$ for all $x, y \in Q$

Some other result on algebraic properties of right-sided quasigroup were deduced by Robinson [2], Stanovsky was involved in some works, see [14-17] on distributive quasigroup, so also is Elhamdadi [18], and Stanovsky [5, 19] carried out an overview of the theory of self distributive quasigroups, both in the two-sided and one-sided cases, and related the older results to the modern theory of quandles (which is of application to the Reidemeister moves in Knot theory), to which self-distributive quasigroups are a special case. Much attention was paid to the representation results (loop isotopy, linear and homogeneous representations), as the main tool to investigate self-distributive quasigroups.
In this study, holomorph of a left-right sided quasigroup is considered by first considering the holomorph of distributive quasigroup and quasigroup with the key laws.

2 Main Result

$E(Q, \cdot)$ will be considered as a subsemigroup of the endomorphism semigroup of Q for a quasigroup $(Q, \cdot)$.

Lemma 2.1. Let $E(Q, \cdot)$ be a subsemigroup of the endomorphism semigroup of Q for the quasigroup $(Q, \cdot)$. Let $H(Q) = E(Q) \times Q$ be defined by

$$content...(\alpha, x) \circ (\beta, y) = (\alpha\beta, x\beta \cdot y) \tag{2.1}$$

for all $(\alpha, x), (\beta, y) \in H$, then $(H, \circ)$ is a groupoid.

IJMAO

International Journal of Mathematical Analysis and Optimization: Theory and Applications
Vol. 2019, No. 1, pp. 426 - 432

Remark 2.1. If $E(Q)$ is a submonoid of endomorphism semigroup of Q of a quasigroup $(Q,\cdot)$, then the quasigroup $(H,\circ)$, constructed above, is called the $E(Q)$-holomorph of $(Q,\cdot)$.
Using equation(2.1), Lemma (1.1) and definition (1.2) above, one establishes the following:

Theorem 2.1. Let $E(Q)$ be a subsemigroup of the endomorphism semigroup of Q for a quasigroup $(Q,\cdot)$. Then $H(Q)$ is a left distributive groupoid (LDG) if and only if $E(Q)$ is left distributive and the identity

$$x\beta\gamma\cdot(y\gamma\cdot z)=(x\beta\cdot y)\alpha\gamma\cdot(x\gamma\cdot z)$$

holds for all α, β, $\gamma\in E(Q)$ and $x,y,z\in Q$.
Proof: Suppose $H(Q)$ is a left distributive groupoid (LDG), then,

$$(\alpha,x)\circ[(\beta,y)\circ(\gamma,z)]=[(\alpha,x)\circ(\beta,y)]\circ[(\alpha,x)\circ(\gamma,z)]$$

$$(\alpha,x)\circ(\beta\gamma,y\gamma\cdot z)=(\alpha\beta,x\beta\cdot y)\circ(\alpha\gamma,x\gamma\cdot z)$$

$$(\alpha\beta\gamma,x\beta\gamma\cdot(y\gamma\cdot z))=\Big(\alpha\beta\alpha\gamma,(x\beta\cdot y)\alpha\gamma\cdot(x\gamma\cdot z)\Big) \tag{2.2}$$

Equation (2.2) is true if and only if

$$\alpha\beta\gamma=\alpha\beta\alpha\gamma \tag{2.3}$$

and

$$x\beta\gamma\cdot(y\gamma\cdot z)=(x\beta\cdot y)\alpha\gamma\cdot(x\gamma\cdot z). \tag{2.4}$$

Conversely, suppose $E(Q)$ is left distributive and the identities hold , then

$$\alpha\beta\gamma=\alpha\beta\alpha\gamma \tag{2.5}$$

and

$$x\beta\gamma\cdot(y\gamma\cdot z)=(x\beta\cdot y)\alpha\gamma\cdot(x\gamma\cdot z). \tag{2.6}$$

Combining equations (2.5) and (2.6) to obtain

$$(\alpha\beta\gamma,x\beta\gamma\cdot(y\gamma\cdot z))=\Big(\alpha\beta\alpha\gamma,(x\beta\cdot y)\alpha\gamma\cdot(x\gamma\cdot z)\Big) \tag{2.7}$$

which splits into

$$(\alpha,x)\circ[(\beta,y)\circ(\gamma,z)]=[(\alpha,x)\circ(\beta,y)]\circ[(\alpha,x)\circ(\gamma,z)]$$

when equation (2.1) is applied to equation (2.7). Thus, $H(Q)$ is left distributive groupoid. □

Theorem 2.2. Let $E(Q)$ be a subsemigroup of the endomorphism semigroup of Q for a quasigroup $(Q,\cdot))$. Then, $H(Q)$ is a right distributive groupoid (RDG) if and only if $E(Q)$ is right distributive and the identity

$$(y\gamma\cdot z)\alpha\cdot x=(y\alpha\cdot x)\gamma\alpha\cdot(z\alpha\cdot x)$$

holds for all α, β, $\gamma\in E(Q)$ and $x,y,z\in Q$.
Proof: Suppose $H(Q)$ is a right distributive groupoid (RDG), then,

$$[(\beta,y)\circ(\gamma,z)]\circ(\alpha,x)=[(\beta,y)\circ(\alpha,x)]\circ[(\gamma,z)\circ(\alpha,x)]$$

$$(\beta\gamma,y\gamma\cdot z)\circ(\alpha,x)=(\beta\alpha,y\alpha\cdot x)\circ(\gamma\alpha,z\alpha\cdot x)$$

IJMAO

International Journal of Mathematical Analysis and Optimization: Theory and Applications
Vol. 2019, No. 1, pp. 426 - 432

$$\Big(\beta\gamma\alpha, (y\gamma \cdot z)\alpha \cdot x\Big) = \Big(\beta\alpha\gamma\alpha, (y\alpha \cdot x)\gamma\alpha \cdot (z\alpha \cdot x)\Big). \tag{2.8}$$

Equation (2.8) is true if and only if

$$\beta\gamma\alpha = \beta\alpha\gamma\alpha$$

and

$$(y\gamma \cdot z)\alpha \cdot x = (y\alpha \cdot x)\gamma\alpha \cdot (z\alpha \cdot x).$$

Conversely, suppose $E(Q)$ is right distributive and the identity hold that is

$$\beta\gamma\alpha = \beta\alpha\gamma\alpha \tag{2.9}$$

and

$$(y\gamma \cdot z)\alpha \cdot x = (y\alpha \cdot x)\gamma\alpha \cdot (z\alpha \cdot x). \tag{2.10}$$

Combining equations (2.9) and (2.10) to obtain

$$\Big(\beta\gamma\alpha, (y\gamma \cdot z)\alpha \cdot x\Big) = \Big(\beta\alpha\gamma\alpha, (y\alpha \cdot x)\gamma\alpha \cdot (z\alpha \cdot x)\Big) \tag{2.11}$$

which split into

$$[(\beta, y) \circ (\gamma, z)] \circ (\alpha, x) = [(\beta, y) \circ (\alpha, x)] \circ [(\gamma, z) \circ (\alpha, x)]$$

when equation (2.1) is applied to equation (2.11).
Thus, $H(Q)$ is right distributive groupoid. □

Corollary 2.1. $H(Q)$ is distributive groupoid (DG) if and only if $E(Q)$ is distributive and the two identities

$$x\beta\gamma \cdot (y\gamma \cdot z) = (x\beta \cdot y)\alpha\gamma \cdot (x\gamma \cdot z)$$

and

$$(y\gamma \cdot z)\alpha \cdot x = (y\alpha \cdot x)\gamma\alpha \cdot (z\alpha \cdot x)$$

hold for all α, β, $\gamma \in E(Q)$ and $x, y, z \in Q$.
Proof: From Theorem 2.1 and Theorem 2.2., the result follows. □

Theorem 2.3. $H(Q)$ has the left key law (LKL) if and only if $E(Q)$ has the left key law (LKL) and the identity

$$x\alpha\beta \cdot (x\beta \cdot y) = y$$

holds for all α, $\beta \in E(Q)$ and $x, y \in Q$.
Proof: $H(Q)$ has the left key law (LKL) if and only if

$$(\alpha, x) \circ [(\alpha, x) \circ (\beta, y)] = (\beta, y)$$

$$\iff (\alpha, x) \circ (\alpha\beta, x\beta \cdot y) = (\beta, y)$$

$$\iff (\alpha\alpha\beta, x\alpha\beta \cdot (x\beta \cdot y)) = (\beta, y)$$

$$\iff \alpha\alpha\beta = \beta$$

and

$$x\alpha\beta \cdot (x\beta \cdot y) = y.$$

Hence, the result follows. □

IJMAO

International Journal of Mathematical Analysis and Optimization: Theory and Applications
Vol. 2019, No. 1, pp. 426 - 432

Theorem 2.4. $H(Q)$ has the right key law (RKL) if and only if $E(Q)$ has the right key law (RKL)and the identity

$$(y\alpha \cdot x)\alpha \cdot x = y$$

holds for all $\alpha \in E(Q)$ and $x, y \in Q$.
Proof: $H(Q)$ has the right key law (RKL) if and only if

$$[(\beta, y) \circ (\alpha, x)] \circ (\alpha, x) = (\beta, y)$$
$$\iff (\beta\alpha, y\alpha \cdot x) \circ (\alpha, x) = (\beta, y)$$
$$\iff (\beta\alpha\alpha, (y\alpha \cdot x)\alpha \cdot x) = (\beta, y)$$
$$\iff \beta\alpha\alpha = \beta$$

and

$$(y\alpha \cdot x)\alpha \cdot x = y.$$

Hence, the result follows. □

Theorem 2.5. $H(Q)$ is left-sided if and only if $E(Q)$ is left-sided and the identities

$$x\beta\gamma \cdot (y\gamma \cdot z) = (x\beta \cdot y)\alpha\gamma \cdot (x\gamma \cdot z) \text{ and } x\alpha\beta \cdot (x\beta \cdot y) = y$$

hold for all α, β, $\gamma \in E(Q)$ and $x, y, z \in Q$.
Proof: $H(Q)$ is left-sided if and only if $H(Q)$ is a left distributive groupoid and $H(Q)$ has the left key law. Going by Theorem 2.1 and Theorem 2.2, $H(Q)$ is left-sided if and only if the identity

$$x\alpha\beta \cdot (x\beta \cdot y) = y$$

and the identity

$$x\beta\gamma \cdot (y\gamma \cdot z) = (x\beta \cdot y)\alpha\gamma \cdot (x\gamma \cdot z)$$

hold for all α, β, $\gamma \in E(Q)$ and $x, y, z \in Q$. □

Theorem 2.6. $H(Q)$ is right-sided if and only if $E(Q)$ is right-sided and the identities

$$(y\gamma \cdot z)\alpha \cdot x = (y\alpha \cdot x)\gamma\alpha \cdot (z\alpha \cdot x) \text{ and } (y\alpha \cdot x)\alpha \cdot x = y$$

hold for all α, β, $\gamma \in E(Q)$ and $x, y, z \in Q$.
Proof: $H(Q)$ is right-sided if and only if $H(Q)$ is a right distributive groupoid and $H(Q)$ has the right key law. Going by Theorem 2.2 and Theorem 2.4, $H(Q)$ is right-sided if and only if the identity

$$[(\beta, y) \circ (\gamma, z)] \circ (\alpha, x) = [(\beta, y) \circ (\alpha, x)] \circ [(\gamma, z) \circ (\alpha, x)]$$

and the identity

$$(y\alpha \cdot x)\alpha \cdot x = y$$

hold for all α, β, $\gamma \in E(Q)$ and $x, y, z \in Q$. □

Corollary 2.2. $H(Q)$ is left-right sided if and only if $E(Q)$ is left-right sided and the identities

$$x\beta\gamma \cdot (y\gamma \cdot z) = (x\beta \cdot y)\alpha\gamma \cdot (x\gamma \cdot z) \text{ and } x\alpha\beta \cdot (x\beta \cdot y) = y,$$

$$(y\gamma \cdot z)\alpha \cdot x = (y\alpha \cdot x)\gamma\alpha \cdot (z\alpha \cdot x) \text{ and } (y\alpha \cdot x)\alpha \cdot x = y$$

hold for all α, β, $\gamma \in E(Q)$ and $x, y, z \in Q$.

Proof: From Theorem 2.3. and Theorem 2.4., the result follows. □

IJMAO

International Journal of Mathematical Analysis and Optimization: Theory and Applications
Vol. 2019, No. 1, pp. 426 - 432

3 Applications

The left (right) key laws in the holomorph of a quasigroup can be used for symmetric cryptography (secret key cryptosystem) based on Theorem 2.3 and Theorem 2.4 as discussed below.

Based on Theorem 2.3 Let the plain text be y and let there be a repository $E(Q) \times H(Q) = E(Q) \times E(Q) \times Q$ of keys in the triple form (α, β, x). Let us assume that the sender is Samson, while the receiver is Tope. It is assumed that Samson and Tope already share the repository of key prior to communication. Samson will encrypt the plain text y with the key $x\beta$ to get the cipher text $x\beta \cdot y$ which will be sent to Tope. Tope will use the key $x\alpha\beta$ to decrypt the cipher text $x\beta \cdot y$ by computing $x\alpha\beta \cdot (x\beta \cdot y)$ to get the plain text y. Based on the fact that it is important for keys to be changed regularly to prevent any attack on the system, then, an alternative key in the triple form (α', β', x') can be adopted. The quasigroup structure of $(Q, \cdot)$ and groupoid structure of $E(Q)$ give no room for the equality of the triples (α, β, x) and (α', β', x') whenever any one or two of their corresponding components are the same.

Based on Theorem 2.4 Let the plain text be y and let there be a repository $H(Q) = E(Q) \times Q$ of keys in the pair form (α, x). Let us assume that the sender is Samson, while the receiver is Tope. It is assumed that Samson and Tope already share the repository of key prior to communication. Samson will encrypt the plain text y with the key (α, x) to get the cipher text $y\alpha \cdot x$ which will be sent to Tope. Tope will use the key (α, x) to decrypt the cipher text $y\alpha \cdot x$ by computing $(y\alpha \cdot x)\alpha \cdot x$ to get the plain text y. Based on the fact that it is important for keys to be changed regularly to prevent any attack on the system, then, an alternative key in the pair form (α', x') can be adopted. The quasigroup structure of $(Q, \cdot)$ and groupoid structure of $E(Q)$ give no room for the equality of the triples (α, x) and (α', x') whenever any one of their corresponding components are the same.

References

[1] Bruck, R. H. Some results in the theory of quasigroups. *Trans. Amer. Math. Soc.*, **55**(1): 19–52 (1944).

[2] Robinson, D. A. Bol loops. PhD thesis, University of Winsconsin, (1964).

[3] Chiboka, V. O. and Solarin, A. R. T. Holomorphs of conjugacy closed loops. *Scientific Annals of A. I. I. Cuza. Univ.* 37(3), 277–284 (1991).

[4] Pflugfelder, H. O. Quasigroups and Loops: Introduction. *Sigma Series in Pure Mathematics*, **7**, Heldermann Verlag, Berlin (1990).

[5] Stanovsky, D. A guide to self-distributive quasigroups, or latin quandles. *Quasigroups and Related Systems*, **23**, 91–128 (2015).

[6] Robinson, D. A. Holomorphy Theory of Extra Loops. *Publ. Math.Debrecen.*, **18**, 59-64 (1971).

[7] Adéníran, J. O., Jaiyéọlá, T. G., Idowu, K. A. Holomorph of Generalised Bol loops. *Noovi Sad. J. Math.*, **44**(1), 37–51 (2014).

[8] Jaiyéọlá, T. G. An holomorphic study of the Smarandache concept in loops. *Scientia Magna Journal*, **2** (1), 1–8 (2006).

[9] Jaiyéọlá, T.G. An holomorphic study of Smarandache automorphic and cross inverse property loops. In Proceedings of the 4th International Conference on Number Theory and Smarandache Problems. *Scientia Magna Journal*, **4**(1), 102–108 (2008).

[10] Isere, A., Adéníran, J.O. and Jaiyéọlá, T.G. Holomorphy of Osborn loops. *Analele Universitatii De Vest Din Timisoara, Seria Matematica-Informatica*, **53**(2), 81—98 (2015). https://doi.org/10.1515/awutm-2015-0016

[11] Jaiyéọlá, T. G. and Popoola, B. A. Holomorph of generalized Bol loops II, Discussiones Mathematicae-General Algebra and Applications, 35, 1, 59—78 (2015). DOI:10.7151/dmgaa.1234

[12] Jaiyéọlá, T. G., David, S. P., Ilojide E. and Oyebo, Y. T. Holomorphic structure of middle Bol loops. *Khayyam Journal of Mathematics*, **3**(2), 172-–184 (2017). DOI:10.22034/kjm.2017.51111

[13] Jaiyéọlá, T. G. A study of new concepts in smarandache quasigroups and loops. ProQuest Information and Learning(ILQ), Ann Arbor, USA (2009).

[14] Donovan, D. M., Griggs, T. S., McCourt, T. A., Opršal, J., Stanovský, D. Distributive and anti-distributive Mendelsohn triple systems, *Canad. Math. Bull.* **59**(1), 36 —49 (2016).

[15] Hulpke, A., Stanovský, D., Vojtěchovský, P. Connected quandles and transitive groups. *J. Pure Appl. Algebra*, **220**(2), 735-–758 (2016).

[16] Jedlička, P., Pilitowska, A., Stanovský, D., Zamojska-Dzienio, A. The structure of medial quandles. *J. Algebra,* **443** , 300-–334 (2015).

[17] Jedlička, Stanovský, D. and Vojtěchovský, P., Distributive and Trimedial Quasigroups of Order 243, pre-print.

[18] Elhamdadi, M. Distributivity in quandles and quasigroups. *Algebra, geometry and mathematical physics, Springer Proc. Math. Stat.*, **85**, Springer, Heidelberg, 325–340 (2014).

[19] Stanovsky, D. On varieties of left distributive left idempotent groupoids. *Discussiones Math. - General Algebra and Appl.*, **24** (2), 267–275 (2004).