On semi-symmetric (α, β, γ)-inverse quasigroup

Richard Ilemobade
(Obafemi Awolowo University, Ile Ife, Nigeria)
E-mail: richardilemobade@gmail.com

Temitope Gbolahan Jaiyeola
(University of Lagos, Akoka, Nigeria and Obafemi Awolowo University, Ile Ife, Nigeria)
E-mail: tgjaiyeola@unilag.edu.ng, tjayeola@oauife.edu.ng

Quasigroups and loops are generalizations of groups (see [2, 9, 10]).

Definition 1. Let $(Q, \cdot)$ be a system of non-empty set Q and a binary operation $(\cdot)$. $(Q, \cdot)$ will be called a quasigroup if for $a, b \in Q$, the equations $a \cdot x = b$ and $y \cdot a = b$ have unique solutions $(x, y) \in Q \times Q$.

Definition 2. A quasigroup $(Q, \cdot)$, in which there is a unique element $\mu \in Q$, such that $x \cdot \mu = x = \mu \cdot x \ \ \forall\, x \in Q$, is called a loop. The element μ is called the identity element in Q.

In associative algebraic systems, the notion of an inverse element or property holds significance only when the system possesses a neutral element, as seen in groups, for instance. Nevertheless, in quasigroups, the inverse property can be meaningfully established even when there is no neutral element present.

Definition 3. A quasigroup $(Q, \cdot)$ will be said to have the inverse property if there are permutations on Q: $J_\lambda : x \longrightarrow x^\lambda$ and $J_\rho : x \longrightarrow x^\rho$ such that $x^\lambda(xy) = y$ and $(yx)x^\rho = y$ for $x, y \in Q$.

Certain varieties of quasigroups or loops lack the inverse property, yet exhibit characteristics that can be viewed as variations of the inverse property.

Definition 4. A quasigroup $(Q, \cdot)$ has the cross-inverse-property (and is called a CIP quasigroup) if there exists a permutation $J : \ Q \to Q;\ x \longmapsto xJ$ such that either of the following holds: $(x \cdot y) \cdot xJ = y$ or $xJ \cdot (y \cdot x) = y$ for all $x,\, y \in Q$. If $(Q, \cdot)$ is a loop with the neutral element μ, then $J = J_\lambda$ or $J = J_\rho$ and we have a CIP loop.

This class of quasigroup and loop, and their generalizations have been studied and found to be applicable to cryptography (see [7, 3]). Among such generalizations is the m-inverse quasigroup and loop (see [4]) .

Definition 5. If there is a permutation J of elements of a quasigroup $(Q, \cdot)$ such that $\forall\ x, y \in Q$ $(x \cdot y)J^m \cdot xJ^{m+1} = yJ^m$, where m is an integer, then $(Q, \cdot)$ is called an m-inverse quasigroup. In the special case $(Q, \cdot)$ is a loop with neutral element μ and $x \cdot xJ = \mu$ for all $x \in Q$, then we have an m-inverse loop.

Another of such is the (r, s, t)-inverse quasigroup (see [1, 5, 6]) which (α, β, γ)-inverse quasigroup generalizes.

Definition 6. If there is a permutation J of elements of a quasigroup $(Q, \cdot)$ such that $\forall\ x, y \in Q$ $(x \cdot y)J^r \cdot xJ^s = yJ^t$, where r, s and t are integers, then $(Q, \cdot)$ is called an (r, s, t)-inverse quasigroup. If in addition, $(Q, \cdot)$ is a loop and the permutation J is such that $x \cdot xJ = \mu$, where μ is the neutral element in Q, then $(Q, \cdot)$ is an (r, s, t)-inverse loop.

A quasigroup $(Q, \cdot)$ will be called an (α, β, γ)-inverse quasigroup, if there exist fixed permutations α, β and γ of Q, such that $(x \cdot y)\alpha \cdot x\beta = y\gamma \ \ \forall\ (x, y) \in Q \times Q$.

Conjecture 7. *A quasigroup can have more than one triple of bijections* (α, β, γ)*, for which the* (α, β, γ)*-inverse property holds.*

In this work, examples were given to illustrate that a quasigroup can have more than one (α, β, γ)-inverse property.

Definition 8. Let $(Q, \cdot)$ be a quasigroup. Define the set Δ_Q as follows:

$$\Delta_Q := \{\omega = \langle \alpha, \beta, \gamma \rangle : (x \cdot y)\alpha \cdot x\beta = y\gamma, \ x, y \in Q\}$$

where α, β, and γ are permutations of Q.

Definition 9. A quasigroup $(Q, \cdot)$ is said to be semi-symmetric if it satisfies the identity $(x \cdot y) \cdot x = y$ for all $x, y \in Q$.

For non-empty set Δ_Q of quasigroup $(Q, \cdot)$, it was shown that if the semi-symmetry law holds in $(Q, \cdot)$, it induces a binary operation on Δ_Q for which Δ_Q is a group.

Theorem 10. *Let* $(Q, \cdot)$ *be an* (α, β, γ)*-inverse quasigroup. If* $(Q, \cdot)$ *is semi-symmetric, then there exists a binary operation* $\otimes$ *on* Δ_Q*, such that* $(\Delta_Q, \otimes)$ *is a group.*

Conjecture 11. *There is relationship between* Δ_Q *and the autotopism group* $ATP(Q)$*, for a quasigroup* $(Q, \cdot)$*.*

Interestingly, this relation is actually an isomorphism between Δ_Q and the autotopism group of $(Q, \cdot)$.

Theorem 12. *For an* (α, β, γ)*-inverse quasigroup* $(Q, \cdot)$ *that is semi-symmetric,* $(\Delta_Q, \otimes)$ *and* $ATP(Q)$ *are isomorphic i.e* $\Delta_Q \cong ATP(Q)$*.*

References

[1] R. Ilemobade, O. George and T.G. Jaiyeola. On the universality and isotopy-isomorphy of (r, s, t)-inverse quasigroups and loops with applications to cryptography. *Quasigroup and Related Systems*, 31: 53–64, 2023.

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

[3] A. D. Keedwell. Crossed-inverse quasigroups with long inverse cycles and applications to cryptography. *Australas. J. Combin.*, 20: 241–-250, 1999.

[4] A. D. Keedwell and V. A. Shcherbacov. On m-inverse loops and quasigroups with a long inverse cycle. *Australas. J. Combin.*, 26: 99–-119, 2002.

[5] A. D. Keedwell and V. A. Shcherbacov. Construction and properties of (r, s, t)-inverse quasigroups I. *Discrete Math.*, 266: 275–-291, 2003.

[6] A. D. Keedwell and V. A. Shcherbacov. Construction and properties of (r, s, t)-inverse quasigroups II. *Discrete Math.*, 288: 61-–71, 2004.

[7] A.D. Keedwell and V.A. Shcherbacov. Quasigroups with an inverse property and generalized parastrophic identities. *Quasigroups and Related Systems*, 13: 109–124, 2005.

[8] Y.T. Oyebo, T. G. Jaiyéọlá and J. O. Adeniran. A study of the holomorphy of (r, s, t)-inverse loops, *Journal of Discrete Mathematical Sciences & Cryptography*, 26(1): 67–-86, 2023. https://doi.org/10.1080/09720529.2021.1885810

[9] V. A. Shcherbacov. *Elements of quasigroup theory and applications*, Monographs and Research Notes in Mathematics. CRC Press, Boca Raton, FL, 2017.

[10] A.R.T. Solarin, J.O. Adeniran, T.G. Jaiyeola, A.O. Isere and Y.T. Oyebo. *Some varieties of loops (Bol-Moufang and non-Bol-Moufang types)*. In: Hounkonnou, M.N., Mitrović, M., Abbas, M., Khan, M. (eds) Algebra without Borders – Classical and Constructive Nonassociative Algebraic Structures. STEAM-H: Science, Technology, Engineering, Agriculture, Mathematics & Health. Springer, Cham. 2023. https://doi.org/10.1007/978-3-031-39334-1_3