International J.Math. Combin. Vol.2 (2010), 01-06

On the Crypto-Automorphism of the Buchsteiner Loops

J. O. Adéníran

(Department of Mathematics of University, Agriculture, Abeokuta 110101, Nigeria)

Y.T. Oyebo

(Department of Mathematics, Lagos State University, Ojo, Nigeria)

Email: adeniranoj@unaab.edu.ng, oyeboyt@yahoo.com

Abstract: In this study, New identities of Buchsteiner loops were obtained via the principal isotopes. It was also shown that the middle inner mapping T_v^{-1} is a crypto-automorphism with companions v and v^λ. Our results which are new in a way, complement and extend existing results in literatures.

Key Words: Buchsteiner loop, WWIP-inverse loop, automorphism group, crypto-automorphism.

AMS(2000): 08A05

§1. Introduction

A binary system $(Q, \cdot)$ is called a loop if $a \cdot 1 = a = 1 \cdot a, \forall a \in Q$, and if the equations $ax = b$ and $ya = b$ have respectively unique solutions $x = a \backslash b$ and $y = b/a, \forall a, b \in Q$. The mappings R_x and L_x for each $x \in Q$, called respectively the right and left translation mappings, are defined as $yx = yR_x$ and $xy = yL_x, \forall y \in Q$, they are one-to-one mapping of Q onto Q. It is important to know that the group generated by all these mappings are called multiplication group $MlpQ$, readers should please see [1,10].

Therefore, a loop $(Q, \cdot)$ is called Buchsteiner loop, if $\forall\ x, y, z \in Q$, the identity

$$x \backslash (xy \cdot z) = (y \cdot zx)/x \tag{1.1}$$

is obeyed. This loop was first noticed by Buchsteiner [3] in 1976. Thereafter much is not heard of it until 2004, when Piroska Csögo, et al came up with a comprehensive study on this loop structure [5,6]. In fact, they presented for the first time, an example of Buchsteiner loop which is conjugacy closed.

A Buchsteiner loop is isomorphic to all its loops isotopes, hence it is a G-loop. It is not an inverse property loop, however it satisfies a kind of inverse known as *doubly weak inverse property*(WWIP) [5].

[1]Received April 7, 2010. Accepted May 25, 2010.

A loop $(Q,\cdot)$ is called *doubly weak inverse property* (WWIP) if the identity

$$(x\cdot y)J_\rho\cdot xJ_\rho^2=yJ_\rho \tag{1.2}$$

holds $\forall\ x,y\in Q$. Buchsteiner loop is a is a class of G-loop which is defined concisely by an equation. This makes the study of Buchsteiner loop interesting since G-loop is not known to be described by a first order sentence [5].

These facts, provided the background to obtain some new identities for Buchsteiner loops. These identities, were in turn used to show that T_v^{-1} is a crypto-automorphism with companion v and v^λ.

Definition 1.1 *(1) An isotopism of loops $(Q,\circ)$ and $(,\cdot)$ with same underlying set, is a triple (α,β,γ) of permutation of Q satisfying*

$$x\alpha\cdot y\beta=(x\circ y)\gamma,\forall\ x,y\in Q. \tag{1.3}$$

In this case $(Q,\circ)$ and $(Q,\cdot)$ are said to be isotopic.

*(2)An isotopism (α,β,γ) is called principal if $\gamma=Id_Q$. In such a case $1\in Q$ is identity of $(Q,\circ)$, and if we set $1\alpha=u$ and $1\beta=v$, then (**??**) becomes $x\circ y=x/v\cdot u\backslash y=xR_v^{-1}\cdot yL_u^{-1}$, $\forall x,y\in Q$. Here \ and / are left and right division operation in $(Q,\cdot)$. Then the loop $(Q,\circ)$ is called principal isotope of $(Q,\cdot)$.*

(3) An isotopism (α,β,γ) of a loop $(Q,\cdot)$ onto itself is called autotopism. The set $Atp(Q)$ of all autotopisms of a loop Q is a group.

(4) A permutation α of Q is an automorphism if $\alpha\in Aut(Q)$ or if and only if $(\alpha,\alpha,\alpha)\in Atp(Q)$.

Definition 1.2([4]) *Let $(Q,\cdot)$ be any loop. A permutation C on symmetric group of Q is called crypto-automorphism of Q if there exist m, t in Q, such that for every x, y in Q, we have*

$$(x\cdot m)C\cdot(t\cdot y)C=(x\cdot y)C. \tag{1.4}$$

§2. Preliminaries

Lemma 2.1([5]) *A loop Q satisfy the identity (1.1) if and only if*

$$(L_x^{-1},R_x,L_x^{-1}R_x) \tag{2.1}$$

is an autotopism $\forall\ x\in Q$.

Lemma 2.2([5]) *A loop $(Q,\cdot)$ satisfies the Buchsteiner identity $x\backslash(xy\cdot z)=(y\cdot zx)/x$, if and only if $(L_x^{-1},R_x,L_x^{-1}R_x)\in Atp(Q),\forall\ x,y,z\in Q$.*

Theorem 2.1([5]) *Let Q be a Buchsteiner loop. Then $\forall\ x,y\in Q$, $R_{(x,y)}=[L_x,R_y]=L^{-1}_{(y,x)}$.*

Note also that, the commutator $[L_x,R_y]$, is defined as $L_xR_y=R_yL_x[L_x,R_y]\Rightarrow\ L_x^{-1}R_y^{-1}L_xR_y=[L_x,R_y]\Rightarrow\ L_x^{-1}L_y^{-1}L_{yx}=[L_x,R_y]$, since from Lemma 2.2, $R_y^{-1}L_xR_y=L_y^{-1}L_{yx}$.

Theorem 2.2([2]) *Let $(Q,\cdot,\backslash,/)$ be a quasigroup. If $Q(a,b,\circ)\overset{\theta}{\cong}Q(c,d,*)$, then $Q(f,g,\triangle)\overset{\theta}{\cong}Q((f\cdot b)\theta/d, c\backslash(a\cdot g)\theta,\square)$. If $(Q,\cdot)$ is a loop, then $(f\cdot b)\theta/d=[f\cdot(a\backslash c\theta^{-1})]\theta$ and $c\backslash(a\cdot g)\theta=[(d\theta^{-1}/b)\cdot g]\theta$, where $a,b,c,d,f,g\in Q$.*

§3. Main Results

Our first main result reads:

Theorem 3.1 *A loop $(Q,\cdot,\backslash,/)$ is a Buchsteiner loop if and only if the identity*

$$u\{x\backslash[(xy)/v\cdot z]\}=\{[(uy)/v\cdot u\backslash\{(uz)/v\cdot u\backslash(xv)\}]/(u\backslash(xv))\}v \tag{3.1}$$

holds $\forall u,v,x,y,z\in Q$.

Proof Suppose $(Q,\cdot,\backslash,/)$ is a Buchsteiner loop with any arbitrary principal isotope $(Q,\circ)$ such that $x\circ y=xR_v^{-1}\cdot yL_u^{-1}=x/v\cdot u\backslash y,\forall\ u,v\in Q$. Buchsteiner loops are G-loops [5]. Now choose $u,v\in Q$ such that $(Q,\circ)$ is loop isotope of $(Q,\cdot)$. Therefore, we have $x\backslash[(x\circ y)\circ z]=[y\circ(z\circ x)]/x\ \Rightarrow\ x\backslash[(xR_v^{-1}\cdot yL_u^{-1})R_v^{-1}\cdot zL_u^{-1}]=[yR_v^{-1}\cdot(zR_v^{-1}\cdot xL_u^{-1})L_u^{-1}]/x$. Now choose p such that $x\backslash[(xR_v^{-1}\cdot yL_u^{-1})R_v^{-1}\cdot zL_u^{-1}]=p=[yR_v^{-1}\cdot(zR_v^{-1}\cdot xL_u^{-1})L_u^{-1}]/x$, then $[(xR_v^{-1}\cdot yL_u^{-1})R_v^{-1}\cdot zL_u^{-1}]=x\circ p\Leftrightarrow[yR_v^{-1}\cdot(zR_v^{-1}\cdot xL_u^{-1})L_u^{-1}]=p\circ x$. Solving these two separately and equating the answers give

$$u[(x/v)\backslash\{([(x/v)\cdot(u\backslash y)]/v)\cdot(u\backslash z)\}]=[\{(y/v)\cdot(u\backslash[(z/v)\cdot(u\backslash x)])\}/(u\backslash x)]v$$

Setting $x'=x/v\Rightarrow\ x'v=x$, $y'=u\backslash y\ \Rightarrow\ uy'=y$ and $z'=u\backslash z\Rightarrow\ uz'=z$ in the last expression gives

$$u\{x'\backslash[(x'y')/v\cdot z']\}=\{[(uy')/v\cdot u\backslash\{(uz')/v\cdot u\backslash(x'v)\}]/(u\backslash(x'v))\}v$$

which is the required identity if $x',y'$and $z'$are respectively replaced by x,y and z
Conversely, let $(Q,\cdot)$ be a loop which obeys equation (3.1), working upward the process of the proof of necessary condition, we obtain the Buchsteiner identity relation for any arbitrary u,v-principal isotope $(Q,\circ)$ of $(Q,\cdot)$. □

Lemma 3.1 *Let $(Q,\cdot)$ be a loop. Then*

(1) Q is a Buchsteiner loop if and only if, $\forall\ x,u,v\in Q$, the triple

$$(R_vL_x^{-1}L_uR_v^{-1},L_uR_v^{-1}R_{\{u\backslash(xv)\}}L_u^{-1},L_x^{-1}L_uR_v^{-1}R_{\{u\backslash(xv)\}})\in Atp(Q). \tag{3.2}$$

(2) In particular, Q is a Buchsteiner loop if $\forall u,v\in Q$, the triple

$$(R_vL_uR_v^{-1},L_uR_v^{-1}R_{(u\backslash v)}L_u^{-1},L_uR_v^{-1}R_{(u\backslash v)})\in Atp(Q). \tag{3.3}$$

Proof (1) Suppose the Q is a Buchsteiner loop, then equation (3.1) of Theorem 3.1 holds in $(Q,\cdot)$. Expressing the equation in term of autotopism gives (3.2). Conversely, suppose the autotopism (3.2) holds in Q, $\forall\ u, v \in Q$, taking any $y, z \in Q$ it implies that, $yR_vL_x^{-1}L_uR_v^{-1} \cdot zL_uR_v^{-1}R_{\{u\backslash(xv)\}}L_u^{-1} = (yz)L_x^{-1}L_uR_v^{-1}R_{\{u\backslash(xv)\}}$, the rest is simple.

(2) Suppose the Q is a Buchsteiner loop, then equation (3.1) of Theorem 3.1 holds in $(Q,\cdot)$, hence the autotopism (3.2) holds in Q. The required result is obtained if we set $x = 1$ in this autotopism. □

Theorem 3.2 *Let $(Q,\cdot)$ be a loop, $(Q,\circ)$ an arbitrary principal isotope of $(Q,\cdot)$ and $(Q,*)$ some isotopes of $(Q,\cdot)$. Then $(Q,\cdot)$ is a Buchsteiner loop if and only if the commutative diagram*

$$(Q,\cdot) \xrightarrow[\textit{left principal isotopism}]{(R_v,I,I)} (Q,*) \xrightarrow[\textit{isomorphism}]{(\eta,\eta,\eta)} (Q,\circ) \xrightarrow[\textit{principal isotopism}]{(R^{-1}_{(u\backslash v)},L_u^{-1},I)} (Q,\cdot)$$

holds, where $\eta = L_uR_v^{-1}R_{(u\backslash v)}, \forall u, v \in Q$.

Proof Suppose $(Q,\cdot)$ is a Buchsteiner loop, by Lemma 3.1(2) the autotopism (3.3) holds in $(Q,\cdot)$. Thus, $(R_vL_uR_v^{-1}, L_uR_v^{-1}R_{(u\backslash v)}L_u^{-1}, L_uR_v^{-1}R_{(u\backslash v)}) = (R_v, I, I)(\eta,\eta,\eta)(R^{-1}_{(u\backslash v)}, L_u^{-1}, I)$, where $\eta = L_uR_v^{-1}R_{(u\backslash v)}$. Expressing this in terms of composition supplies the prove of the necessity. Conversely, suppose the commutative diagram holds in Q, we only need to show that the autotopism (3.3) holds in $(Q,\cdot)$. This is obtained by component multiplication of the compositions of the commutative diagram. □

Theorem 3.3 *A Buchsteiner loop $(Q,\cdot,\backslash,/)$ obeys the identities: $((uz)/v)\cdot(u\backslash v) = u\{(u[(u\backslash v)/v\cdot z])/v \cdot (u\backslash v)\}$ and $u\{[u\backslash(yv)]/v\} = \{(y \cdot u\backslash[(u/v)\cdot(u\backslash v)])/(u\backslash v)\}v$.*

Proof From Theorem 3.2, observed that $(Q,\circ)$ and $(Q,*)$ are principal and left principal isotopes of $(Q,\cdot)$ respectively and $\eta = L_uR_v^{-1}R_{(u\backslash v)}$ is an isomorphism. Therefore $(Q,1,v,\circ) \overset{\eta}{\cong} (Q,u,u\backslash v,*)$. Let $(Q,y,z,\triangle)$ be an arbitrary principal isotope of $(Q,\cdot)$, comparing these with the statement of Theorem 2.2, we have $a = 1$, $b = v$, $c = u$, $d = u\backslash v$, $f = y$, $g = z$ and $\theta = \eta = L_uR_v^{-1}R_{(u\backslash v)}$. Using these we can compute: $c\backslash(a\cdot g)\theta = u\backslash(1\cdot z)L_uR_v^{-1}R_{(u\backslash v)} = u\backslash\{((uz)/v)\cdot(u\backslash v)\}$ and $[(d\theta^{-1}/b)\cdot g]\theta = [\{(u\backslash v)(L_uR_v^{-1}R_{(u\backslash v)})^{-1}\}/v\cdot z]L_uR_v^{-1}R_{(u\backslash v)} = \{(u[(u\backslash v)/v\cdot z])/v\}(u\backslash v)$. Hence $c\backslash(a\cdot g)\theta = [(d\theta^{-1}/b)\cdot g]\theta \Leftrightarrow u\backslash\{((uz)/v)\cdot(u\backslash v)\} = \{(u[(u\backslash v)/v\cdot z])/v\}(u\backslash v) \Leftrightarrow ((uz)/v)\cdot(u\backslash v) = u\{(u[(u\backslash v)/v\cdot z])/v\cdot(u\backslash v)\}$, which proved the first identity. The second is similarly obtained, using appropriate arrangement. □.

Corollary 3.1 *Let $(Q,\cdot)$ be a Buchsteiner loop. Then the identities $(vz)/v = v[(v\cdot v^{\lambda}z)/v]$ and $v\{(v\backslash(yv))/v\} = yv^{\rho}\cdot v$ hold $\forall\ v, y, z \in Q$.*

Proof All of these identities are obtained respectively by identities of Theorem 3.3 by setting $u = v$. □

Corollary 3.2 *If $(Q,\cdot)$ is a Buchsteiner loop, then*

(1) $(vz)/v = v[(v\cdot v^{\lambda}z)/v]$ if and only if $L_v^{-1} = T_vL_{v^{\lambda}}T_v^{-1}$, $\forall v, z \in Q$;

(2) $v\{(v\backslash(yv))/v\} = yv^{\rho}\cdot v$ if and only if $R_v = T_v^{-1}R_{v^{\rho}}^{-1}T_v$, $\forall v, y \in Q$.

Proof Setting $u = v$ in the identities of Theorem 3.3, we obtained $(vz)/v = v[(v\cdot v^{\lambda}z)/v] \Rightarrow L_v^{-1} = T_vL_{v^{\lambda}}T_v^{-1}$ from the first one. Conversely, suppose $L_v^{-1} = T_vL_{v^{\lambda}}T_v^{-1}$

holds in Q, now for any $z \in Q$ $zL_v^{-1} = zT_vL_{v^\lambda}T_v^{-1} \Leftrightarrow v\backslash z = \{v[v^\lambda(v\backslash(zv))]\}/v$, now set $z = v\backslash(zv)$ and the first identity is obtained. The second assertion is similarly obtained. □

Corollary 3.3 *Let Q be a Buchsteiner loop, then $(T_vL_{v^\lambda}T_v^{-1}, T_v^{-1}R_{v^\rho}^{-1}T_v, T_vL_{v^\lambda}T_v^{-1}T_v^{-1}R_{v^\rho}^{-1}T_v) \in Atp(Q), \forall v \in Q$.*

Proof This is obtained by substituting the assertion of Corollary 3.2 into the autotopism (2.1). □

Lemma 3.2 *A permutation C on symmetric group of a loop Q is called crypto-automorphism, if and only if $(R_mC, L_tC, C) \in Atp(Q)$, where $m, t \in Q$.*

Proof Suppose C is a crypto-automorphism, then by Definition 1.2 equation (1.4) holds in Q, ie $(x \cdot m)C \cdot (t \cdot y)C = (x \cdot y)C \Leftrightarrow xR_mC \cdot yL_tC = (xy)C \Leftrightarrow (R_mC, L_tC, C) \in Atp(Q)$. Thus the result follows. □

Theorem 3.4 *Let $(Q, \cdot)$ be a Buchsteiner loop. Then*

(1) $T_vL_{(v^\lambda,v)}$ is a crypto-automorphism with companions $v\backslash(v^\rho v)$ and v.

(2) T_v is a crypto-automorphism with companions $v\backslash(v^\rho v)$ and v.

Proof (1)Using the autotopism $A = (T_vL_{v^\lambda}T_v^{-1}, T_v^{-1}R_{v^\rho}^{-1}T_v, T_vL_{v^\lambda}T_v^{-1}T_v^{-1}R_{v^\rho}^{-1}T_v)$ in Corollary 3.3 such that for any $y, z \in Q$, we have

$$yT_vL_{v^\lambda}T_v^{-1} \cdot zT_v^{-1}R_{v^\rho}^{-1}T_v = (yz)T_vL_{v^\lambda}T_v^{-1}T_v^{-1}R_{v^\rho}^{-1}T_v.$$

If we set $z = 1$, we obtain

$$\begin{aligned}
&yT_vL_{v^\lambda}T_v^{-1}R_v = yT_vL_{v^\lambda}T_v^{-1}T_v^{-1}R_{v^\rho}^{-1}T_v \\
&\Leftrightarrow yT_vL_{v^\lambda}L_v = yT_vL_{v^\lambda}T_v^{-1}T_v^{-1}R_{v^\rho}^{-1}T_v \\
&\Leftrightarrow yT_v(L_v^{-1}L_{v^\lambda}^{-1})^{-1} = yT_vL_{v^\lambda}T_v^{-1}T_v^{-1}R_{v^\rho}^{-1}T_v \\
&\Leftrightarrow yT_v(L_v^{-1}L_{v^\lambda}^{-1}L_{v^\lambda v})^{-1} = yT_vL_{v^\lambda}T_v^{-1}T_v^{-1}R_{v^\rho}^{-1}T_v.
\end{aligned}$$

From Theorem 2.1, we have $yT_vL_{(v,v^\lambda)} = yT_vL_{v^\lambda}T_v^{-1}T_v^{-1}R_{v^\rho}^{-1}T_v$. Thus we substitute to get $A = (T_vL_{v^\lambda}T_v^{-1}, T_v^{-1}R_{v^\rho}^{-1}T_v, T_vL_{(v,v^\lambda)})$.

Furthermore, $A^{-1} = (T_vL_{v^\lambda}^{-1}T_v^{-1}, T_v^{-1}R_{v^\rho}T_v, L_{(v,v^\lambda)}^{-1}T_v^{-1})$, thus for any $y, z \in Q$, applying A^{-1} we obtain, $yT_vL_{v^\lambda}^{-1}T_v^{-1} \cdot zT_v^{-1}R_{v^\rho}T_v = (yz)L_{(v,v^\lambda)}^{-1}T_v^{-1}$. Now by appropriate calculation, we can re-write $A^{-1} = (L_{(v,v^\lambda)}^{-1}T_v^{-1}R_{(v\backslash(v^\rho v))}^{-1}, L_{(v^\lambda,v)}^{-1}T_v^{-1}L_v^{-1}, L_{(v^\lambda,v)}^{-1}T_v^{-1}) \Leftrightarrow A = (R_{(v\backslash(v^\rho v))}T_vL_{(v^\lambda,v)}, L_vT_vL_{(v^\lambda,v)}, T_vL_{(v^\lambda,v)})$, which proved (1).

(2)$L_{(v^\lambda,v)}$ has been observed to be an automorphism in Q ([5]). Thus taking any $a, b \in Q$, we can write from (1) that

$$\begin{aligned}
A &= (R_{(v\backslash(v^\rho v))}T_vL_{(v^\lambda,v)}, L_vT_vL_{(v^\lambda,v)}, T_vL_{(v^\lambda,v)}) \\
&= (R_{(v\backslash(v^\rho v))}T_v, L_vT_v, T_v)(L_{(v^\lambda,v)}, L_{(v^\lambda,v)}, L_{(v^\lambda,v)})
\end{aligned}$$

and the result follows immediately. □

Theorem 3.5 *Let Q be a Buchsteiner loop, then T_v^{-1} is a crypto-automorphism with companions v and $v^\lambda, \forall\ v \in Q$.*

Proof From Theorem 3.4(2), we observed that T_v is a crypto-automorphism with companions $(v\backslash(v^\rho v)$ and v, thus by definition it implies that, for any a and b in Q, we have $aR_{(v\backslash(v^\rho v))}T_v \cdot bL_vT_v = (ab)T_v$. Setting $b = a^\rho$, we obtain $aR_{(v\backslash(v^\rho v))}T_v \cdot a^\rho L_vT_v = 1 \Rightarrow R_{(v\backslash(v^\rho v))}T_v = J_\rho L_vT_vJ_\lambda$, using the fact that Q is WWIP loop ([5]). This in terms of autotopism, implies $B = (J_\rho L_vT_vJ_\lambda, L_vT_v, T_v) \in Atp(Q)$, finally by appropriate calculation we have $J_\lambda L_vT_vJ_\rho = T_vR_v^{-1}$, and $L_vT_v = T_vL_{v^\lambda}^{-1}$, re-writing we have $B = (T_vR_v^{-1}, T_vL_{v^\lambda}^{-1}, T_v) \in Atp(Q), \forall\ v \in Q$. The result follows by taking the inverse of B. □

Corollary 3.4 *Any Buchsteiner loop Q is an $A-$loop.*

Proof It is straight forward from Corollary 5.4 in [5] and the preceding theorem. □

Remark 3.1 Since all the inner mappings, i.e. $L_{(u,v)}, R_{(u,v)}$ and T_v have been established to exhibit one form of automorphism or the other, then $(Q, \cdot)$ is an A-loop.

References

[1] R. H. Bruck (1966), *A survey of binary systems*, Springer-Verlag, Berlin-Göttingen-Heidelberg, 185pp.

[2] B.F. Bryant and H. Schneider, Principal loop-isotopes of quasigroups, *Canad. J. Math.* 18(1966), 120-125.

[3] H.H. Buchsteiner, O nekotorom klasse binarnych lup, *Mat. Issled.* 39(1976), 54-66.

[4] R.Capodaglio Di Cocco, On the Isotopism and the Pseudo-Automorphisms of the Loops, *Bollettino U.M.I.* 7(1993), 199-205.

[5] P.Csörgö, A. Drápal and M.K. Kinyon, Buchsteiner loops, Submitted.

[6] P.Csörgö and A. Drápal, Buchsteiner loops and conjugacy closedness, Preprint.

[6] E. Falconer, *Quasigroup Identities Invariant under Isotopy*, Ph.D thesis, Emory University (1969).

[7] T.G. Jaiyeola, *The study of universality of Osborn loops*, Ph.D. thesis, University of Agriculture, Abeokuta, (2008) 256pp.

[8] A.D. Keedwell, The existence of Buchsteiner and conjugacy-closed quasigroups, *European Journal of Combinatorics*, 30(2009) 1382-1385.

[9] H.O. Pflugfelder, Quasigroups and loops: Introduction, *Sigma Series in Pure Math.* 7(1990), Heldermann Verlag, Berlin.