Pseudoautomorphisms and constructions of Moufang loops

Let Q be a loop, $c \in Q$ and g a permutation of Q. Call g a *left pseudoautomorphism* with *companion* c if

$$cg(x) \cdot g(y) = c \cdot g(xy) \quad \text{for all} \quad x, y \in Q.$$

A *right pseudoautomorphism* f with companion d fulfils $f(x) \cdot f(y)d = f(xy)d$. It may happen that a permutation, say h, is both a left and right pseudoautomorphism (in fact this is always the case when Q is Moufang). Then h is called a *pseudoautomorphism*. If h is a pseudoautomorphism, then it may be necessary to distinguish between a *left* companion (corresponding to c) and a *right* companion (corresponding to d). Note that a left pseudoautomorphism may have more than one companion, and that this is true for right pseudoautomorphisms as well.

Denote by $\mathrm{LPs}(Q)$ the set of all (c, f) such that f is a left pseudoautomorphism with companion c, and by $\mathrm{RPs}(Q)$ the set of all (g, d) such that g is a right pseudoautomorphism with companion d.

Both $\mathrm{LPs}(Q)$ and $\mathrm{RPs}(Q)$ may be regarded as groups. To understand this let us first observe that

$$\begin{aligned}(c, g) \in \mathrm{LPs}(Q) &\;\Leftrightarrow\; (L_c g, g, L_c g) \in \mathrm{Atp}(Q); \text{ and}\\ (f, d) \in \mathrm{RPs}(Q) &\;\Leftrightarrow\; (f, R_d f, R_d f) \in \mathrm{Atp}(Q).\end{aligned}$$

The key connection between autotopisms and pseudoautomorphisms follows from a simple observation:

$$(c, g) \in \mathrm{LPs}(Q) \;\Rightarrow\; g(1) = 1 \text{ and } (f, d) \in \mathrm{RPs}(Q) \;\Rightarrow\; f(1) = 1.$$

This is obvious since $cg(x) \cdot g(1) = cg(x)$ for all $x \in Q$. The point is that an autotopism (α, β, γ) with $\alpha(1) = 1$ or $\beta(1) = 1$ yields a pseudoautomorphism. We shall prove:

$$\begin{aligned}&(\alpha, \beta, \gamma) \in \mathrm{Atp}(Q) \text{ and } \beta(1) = 1 \;\Rightarrow\; (\alpha(1), \beta) \in \mathrm{LPs}(Q) \text{ and } \alpha = \gamma = L_{\alpha(1)}\beta;\\ &(\alpha, \beta, \gamma) \in \mathrm{Atp}(Q) \text{ and } \alpha(1) = 1 \;\Rightarrow\; (\alpha, \beta(1)) \in \mathrm{RPs}(Q) \text{ and } \beta = \gamma = R_{\beta(1)}\alpha.\end{aligned}$$

Proof. Assume $\beta(1) = 1$. Setting $y = 1$ in $\alpha(x)\beta(y) = \gamma(xy)$ yields $\alpha = \gamma$. Setting $x = 1$ gives $L_{\alpha(1)}\beta = \alpha$. □

This makes $\mathrm{LPs}(Q)$ a group with unit $(1, \mathrm{id}_Q)$ and operations

$$(c, f)(d, g) = (cf(d), fg) \text{ and } (c, f)^{-1} = (f^{-1}(c\backslash 1), f^{-1}).$$

To see why the operations are defined as stated, observe that

$$\begin{aligned}(L_c f, f, L_c f)(L_d g, g, L_d g) &= (L_c f L_d g, fg, L_c f L_d g),\\ (L_c f, f, L_c f)^{-1} &= (f^{-1}L_c^{-1}, f^{-1}, f^{-1}L_c^{-1}),\end{aligned}$$

$L_c f L_d g(1) = cf(d)$ and $f^{-1}L_c^{-1}(1) = f^{-1}(c\backslash 1)$. Similarly, $\mathrm{RPs}(Q)$ is a group with operations

$$(f, c)(g, d) = (fg, f(d)c) \text{ and } (f, c)^{-1} = (f^{-1}, f^{-1}(1/c)).$$

The group $\mathrm{LPs}(Q)$ is thus isomorphic to the subgroup of $\mathrm{Atp}(Q)$ formed by all $(\alpha, \beta, \gamma) \in \mathrm{Atp}(Q)$ such that $\beta(1) = 1$. The isomorphism sends (α, β, γ) upon $(\alpha(1), \beta)$.

The following observation is obvious but important:

$$(c, \mathrm{id}_Q) \in \mathrm{LPs}(Q) \Leftrightarrow c \in N_\lambda(Q) \text{ and } (\mathrm{id}_Q, d) \in \mathrm{RPs}(Q) \Leftrightarrow d \in N_\rho(Q).$$

Pseudoautomorphisms with two companions. *Let Q be a loop. Suppose that $c, d \in Q$ and that f permutes Q.*

(1) *Assume $(c, f) \in \mathrm{LPs}(Q)$. Then $f^{-1}(c\backslash 1) = 1/f^{-1}(c)$, and $(d, f) \in \mathrm{LPs}(Q) \Leftrightarrow c/d \in N_\lambda(Q)$.*
(2) Assume $(f, c) \in \mathrm{RPs}(Q)$. *Then $f^{-1}(1/c) = f^{-1}(c)\backslash 1$ and $(f, d) \in \mathrm{RPs}(Q) \Leftrightarrow d\backslash c \in N_\rho(Q)$.*

Proof. Suppose that $(c, f) \in \mathrm{LPs}(Q)$. Then $f(y) = cf(f^{-1}(c\backslash 1)) \cdot f(y)$ is equal to $cf(f^{-1}(c\backslash 1) \cdot y)$ for every $y \in Q$. Setting $y = f^{-1}(c)$ and cancelling c yields $1 = f(f^{-1}(c\backslash 1) \cdot f^{-1}(c))$. Thus $1 = f^{-1}(c\backslash 1) \cdot f^{-1}(c)$ and $f^{-1}(c\backslash 1) = 1/f^{-1}(c)$.

Suppose now that (d, f) also belongs to $\mathrm{LPs}(Q)$. Then $(c, f) \cdot (f^{-1}(d\backslash 1), f^{-1}) = (c(d\backslash 1), \mathrm{id}_Q) \in \mathrm{LPs}(Q)$ as well. Hence $n = c(d\backslash 1) \in N_\lambda(Q)$. Recall that n is an LIP element. Therefore $d(d\backslash 1) = 1 = n^{-1}(c(d\backslash 1)) = (n^{-1}c)(d\backslash 1)$, implying $n^{-1}c = d$, $c = nd$ and $n = c/d$.

If $n = c/d \in N_\lambda(Q)$, then $n^{-1}c = d$ and $(L_n^{-1}L_c f, f, L_n^{-1}L_c f) \in \mathrm{Atp}(Q)$. This yields $(d, f) \in \mathrm{LPs}(Q)$ since $L_n^{-1}L_c f(1) = n^{-1}c = d$. □

When a pseudoautomorphism is an automorphism. *If $(c, f) \in \mathrm{LPs}(Q)$, then $f \in \mathrm{Aut}(Q)$ if and only if $c \in N_\lambda(Q)$. If $(f, c) \in \mathrm{RPs}(Q)$, then $f \in \mathrm{Aut}(Q)$ if and only if $c \in N_\rho(Q)$.*

Proof. Note that $f \in \mathrm{Aut}(Q) \Leftrightarrow (1, f) \in \mathrm{LPs}(Q) \Leftrightarrow (f, 1) \in \mathrm{RPs}(Q)$. □

Companions and the inverse property. *Let Q be an IP loop. Then $(c, f) \in \mathrm{LPs}(Q)$ if and only if $(f, c^{-1}) \in \mathrm{RPs}(Q)$. If $(c, f) \in \mathrm{LPs}(Q)$, then $f(x^{-1}) = (f(x))^{-1}$, for every $x \in Q$.*

Proof. Suppose that $(c, f) \in \mathrm{LPs}(Q)$. Setting $y = x^{-1}$ in $cf(xy) = cf(x) \cdot f(y)$ gives $c = cf(x) \cdot f(x^{-1})$. Since Q is an IP loop, $c = cf(x) \cdot (f(x))^{-1}$. Hence $(f(x))^{-1} = f(x^{-1})$ for every $x \in Q$. Inverting $cf(x^{-1}y^{-1}) = cf(x^{-1}) \cdot f(y^{-1})$ therefore yields $f(y) \cdot f(x)c^{-1} = f(yx)c^{-1}$. □

Commutators and associators. Let Q be a loop. If $x, y \in Q$, then $[x, y] = (yx)^{-1}(xy)$ is called the *commutator* of x and y. If Q is diassociative, then the commutator may be bracketed in any way that respects the order of variables. To get a direct proof of this fact for Moufang loops note that $(x^{-1}y^{-1})(xy) = x^{-1}(y^{-1} \cdot xy)$ since $x((x^{-1}y^{-1}) \cdot xy) = (x(x^{-1}y^{-1})x)y = y^{-1}x \cdot y$ and $y^{-1} \cdot xy = y^{-1}x \cdot y$ as $y^{-1}(xy)y^{-1} = y^{-1}x$. The remaining equalities may be obtained by mirroring.

If $x, y, z \in Q$, then $[x, y, z] = (x \cdot yz)\backslash(xy \cdot z)$ is called the *associator* of x, y and z.

Standard generators in a Moufang loop. *Suppose that x and y are elements of a Moufang loop Q. Then* $\mathrm{RPs}(Q)$ *contains*

$$(R_x^{-1}L_x, x^3),\ (L_{xy}^{-1}L_xL_y, [y^{-1}, x^{-1}]),\ (R_{yx}^{-1}R_xR_y, [x, y]) \text{ and } ([L_x, R_y], [y, x^{-1}]).$$

Furthermore, $L_{xy}^{-1}L_xL_y = [R_x^{-1}, L_y]$ and $R_{yx}^{-1}R_xR_y = [L_x^{-1}, R_y]$.

Proof. Since (R_z^{-1}, L_zR_z, R_z) and (L_z, R_z, L_zR_z) are autotopisms for each $z \in Q$, there are also autotopisms

$$(R_x^{-1}L_x, L_xR_x^2, R_xL_xR_x) \text{ and } (L_{xy}^{-1}L_xL_y, R_{xy}^{-1}R_xR_y, M_{xy}^{-1}M_xM_y),$$

where $M_z = L_zR_z$. Now, $L_xR_x^2(1) = x^3$ and $R_{xy}^{-1}R_xR_y(1) = (yx)(y^{-1}x^{-1}) = [y^{-1}, x^{-1}]$. Hence both $(R_x^{-1}L_x, x^3)$ and $(L_{xy}^{-1}L_xL_y, [y^{-1}, x^{-1}])$ belong to $\mathrm{RPs}(Q)$.

Further autotopisms are

$$(L_{yx}^{-1}L_xL_y, R_{yx}^{-1}R_xR_y, -) \text{ and } ([L_x, R_y], R_x^{-1}M_yR_xM_y^{-1}, -),$$

with $L_{yx}^{-1}L_xL_y(1) = (yx)^{-1}(xy) = [x,y]$ and $R_x^{-1}M_yR_xM_y^{-1}(1) = R_x^{-1}(y\cdot y^{-2}x\cdot y) = R_x^{-1}(y^{-1}x\cdot y) = [y,x^{-1}]$. The former case yields $([x,y], R_{yx}^{-1}R_xR_y) \in \mathrm{LPs}(Q)$. Hence $(R_{yx}^{-1}R_xR_y, [y,x]) \in \mathrm{RPs}(Q)$.

The equation $xy\cdot zx = x\cdot yz\cdot x$ implies $L_{xy} = M_xL_yR_x^{-1}$ and $R_{zx} = M_xR_zL_x^{-1}$. Hence $L_{xy}^{-1}L_xL_y = R_xL_y^{-1}M_x^{-1}L_xL_y = [R_x^{-1}, L_y]$. Proceeding in the mirror way yields $R_{zx}^{-1}R_xR_z = L_xR_z^{-1}M_x^{-1}R_xR_z = [L_x^{-1}, R_z]$. □

Associators and the right nucleus. Recall that the associator $[x,y,z]$ is defined as $(x\cdot yz)\backslash(xy\cdot z)$. There is certain amount of arbitrary decision in this definition. Each of / and \ is eligible to use, and there is no obvious reason for the order of $x\cdot yz$ and $xy\cdot z$. However, this is not a big deal since associators are nearly always used in situations when the way of their definition matters much less than it might have been expected.

Suppose that x, y and z are elements of a loop Q. If $[x,y,z] \in N_\rho(Q)$, then

$$z = L_{xy}^{-1}L_xL_y(z)\cdot[x,y,z].$$

Proof. Multiplying the equality to be proved by xy upon the left yields

$$xy\cdot z = (xy)(((xy)\backslash(x\cdot yz))[x,y,z]).$$

Since $[x,y,z] \in N_\rho(Q)$, the right hand side is equal $(x\cdot yz)[x,y,z]$. The equation $xy\cdot z = (x\cdot yz)[x,y,z]$ is true since this is the definition of $[x,y,z]$. □

The above statement has a number of variations and extensions. However, at this point a detailed treatment will be restricted only to the case of loops Q that are of nilpotency class two. For such a loop there exist abelian groups $(G,+)$ and $(Z,\cdot)$ such that $Z \le Z(Q)$ and $(Q/Z,\cdot) \cong (G,+)$. The operation in Q is thus written multiplicatively, while in Q/Z additively. The situation that is of main interest is that of $Z = Z(Q)$. However, for formal reasons it is better to assume that $Z \le Z(Q)$ and Q/Z is abelian.

Associators and commutators as mappings between two abelian groups. Let $(G,+)$ and $(Z,\cdot)$ be abelian groups such that $Q/Z = G$ and $Z \le Z(Q)$, where Q is a loop. *Then there exist mappings $C\colon G\times G\to Z$ and $A\colon G\times G\times G\to Z$ such that for all $u,v,w\in Q$:*

$$[u,v] = z \;\Leftrightarrow\; C(uZ,vZ) = z \quad\text{and}\quad [u,v,w] = z \;\Leftrightarrow\; A(uZ,vZ,wZ) = z.$$

Proof. Consider $u,v,w \in Q$ and put $z = [u,v,w]$. Thus $(u\cdot vw)z = uv\cdot w$. If $a,b,c \in Z(Q)$, then clearly $(ua(vb\cdot wc))z = (ua\cdot vb)wc$. The case of the commutator is similar. □

Associators, commutators and inner mappings. *Let Q, G, Z, C and A be as above. If $u,v,w\in Q$, then $C(uZ,vZ)\cdot C(vZ,uZ) = 1$,*

$$\begin{aligned}
R_u^{-1}L_u(v) &= v\cdot C(uZ,vZ),\\
L_{uv}^{-1}L_uL_v(w) &= w\cdot A(uZ,vZ,wZ)^{-1},\\
R_{vu}^{-1}R_uR_v(w) &= w\cdot A(wZ,vZ,uZ),\\
[L_u,R_v](w) &= w\cdot A(uZ,wZ,vZ)^{-1} \text{ and}\\
[R_v,L_u](w) &= w\cdot A(uZ,wZ,vZ).
\end{aligned}$$

Proof. Suppose first that $vu\cdot z = uv$. Then $uv\cdot z^{-1} = vu$, $z = C(uZ,vZ)$ and $z^{-1} = C(vZ,uZ)$.

Suppose now that $z\in Q$ is such that $R_u^{-1}L_u(v) = vz$. Then $z\in Z$ and $(uv)/u = vz$ yields $uv = vu\cdot z$.

The case of $L_{uv}^{-1}L_uL_v(w)$ follows from a result above. If $z \in Q$ is such that $R_{vu}^{-1}R_uR_v(w) = wz$, then $z \in Z$ and $wv \cdot u = wz \cdot vu = (w \cdot vu)z$. Hence $z = (w \cdot vu)\backslash(wv \cdot u) = [w, v, u]$.

If $[L_u, R_v](w) = wz$, then $u \cdot wv = (u \cdot wz)v = (uw \cdot v)z$ and $z^{-1} = [u, w, v]$. □

Associators and automorphic inner mappings. *Let Q, G, Z and A be as above.*

(1) *If $L_{xy}^{-1}L_xL_y \in \mathrm{Aut}(Q)$ for all $x, y \in Q$, then $A(a, b, c + d) = A(a, b, c) \cdot A(a, b, d)$ for all $a, b, c, d \in G$.*
(2) *If $R_{yx}^{-1}R_xR_y \in \mathrm{Aut}(Q)$ for all $x, y \in Q$, then $A(a + b, c, d) = A(a, c, d) \cdot A(b, c, d)$ for all $a, b, c, d \in G$.*
(3) *If $[L_x, R_y] \in \mathrm{Aut}(Q)$ for all $x, y \in Q$, then $A(a, b + c, d) = A(a, b, d) \cdot A(a, c, d)$ for all $a, b, c, d \in G$.*

Proof. Let $x, y \in Q$ be such that $L_{xy}^{-1}L_xL_y \in \mathrm{Aut}(Q)$. If $w_1, w_2 \in Q$, then $L_{xy}^{-1}L_xL_y(w_1w_2) = L_{xy}^{-1}L_xL_y(w_1)L_{xy}^{-1}L_xL_y(w_2)$. Therefore

$$w_1w_2 \cdot [x, y, w_1w_2]^{-1} = (w_1 \cdot [x, y, w_1]^{-1})(w_2 \cdot [x, y, w_2]^{-1}).$$

The rest follows from the centrality of associators.

The other cases are similar. □

Moufang loops of nilpotency class two. *Let Q be a loop with a central subloop Z such that $(Q/Z, \cdot) = (G, +)$, where G is an abelian group. Then there exists a mapping $A\colon G \times G \times G \to Z$ such that $A(xZ, yZ, zZ) = [x, y, z]$ for all $x, y, z \in Q$. The loop is Moufang if and only if*

$$A(a, b, c) = A(b, c, a) = A(c, a, b) = A(b, a, c)^{-1} = A(a, c, b)^{-1} = A(c, b, a)^{-1},$$
$$A(a, a, b) = 1 \quad \textit{and} \quad A(a, b, c + d) = A(a, b, c) \cdot A(a, b, d)$$

holds for any choice of $a, b, c, d \in Q$.

An equivalent condition is that

$$A(a, a, b) = A(b, a, a) = 1,\ A(a + b, c, d) = A(a, c, d) \cdot A(b, c, d),$$
$$A(a, b + c, d) = A(a, b, d) \cdot A(a, c, d) \ \textit{and}\ A(a, b, c + d) = A(a, b, c) \cdot A(a, b, d),$$

for all $a, b, c, d \in Q$.

Proof. The former condition on A clearly implies the latter condition. To get the converse implication it suffices to prove $A(a, b, c)^{-1} = A(b, a, c)$ since $A(a, b, c)^{-1} = A(a, c, b)$ may be obtained by a mirror argument. The proof follows from $1 = A(a + b, a + b, c) = A(a, b, c)\,A(b, a, c)\,A(a, a, c)\,A(b, b, c) = A(a, b, c)\,A(b, a, c)$.

If x and y are elements of a Moufang loop Q, then $L_{xy}^{-1}L_xL_y$, $R_{yx}^{-1}R_xR_y$ and $[L_x, R_y]$ are automorphisms since they are pseudoautomorphisms with central companions. Thus $A(a, b, c + d) = A(a, b, c) \cdot A(a, b, d)$, and similarly in the other two cases. The equalities $A(a, a, b) = A(b, a, a) = 1$ follow from the diassociativity (in fact, all that is needed here are the alternative laws).

Let now A fulfil the conditions of the statement. Then $A(-a, b, c) = A(a, b, c)^{-1}$ for all $a, b, c \in G$. Therefore $A(-a, a, b) = 1$, and that implies $(1/x) \cdot xy = (1/x)x \cdot y = y$ for all $x, y \in Q$. That makes Q a LIP loop. The RIP may be be proved by a mirror argument.

This yields $[R_x^{-1}, L_y] = [L_y, R_x]$ since if $z \in Q$, then $[R_x^{-1}, L_y](z) = z \cdot [y, z, x^{-1}]$ and $[L_y, R_x](z) = z \cdot [y, z, x]^{-1}$. Because $L_{xy}^{-1}L_xL_y(z) = z \cdot [x, y, z]^{-1}$, the identity $[L_y, R_x] = L_{xy}^{-1}L_xL_y$ holds as well. Therefore

$$L_{xy}^{-1}L_xL_yR_x = [R_x^{-1}, L_y]R_x = R_xL_y^{-1}R_x^{-1}L_yR_x = R_x[L_y, R_x].$$

Multiplying this equality by $[R_x, L_y]$ upon the right yields $L_{xy}^{-1} L_x R_x L_y = R_x$. That may be written as $L_x R_x L_y = L_{xy} R_x$. And that is the same as the Moufang identity $x(yz \cdot x) = xy \cdot zx$. □

Example of a commutative Moufang loop. Let V be a vector space over a field F. Suppose that $\mathrm{char}(F) = 3$ and $\dim(V) = 3$.

Upon $V \times F$ define a loop Q by

$$(u, a)(v, b) = (u + v, a + b + (u_3 - v_3)(u_1 v_2 - u_2 v_1)),$$

where $u = (u_1, u_2, u_3)$ and $v = (v_1, v_2, v_3)$. This is obviously a commutative loop (in any characteristic) of nilpotence class two. To show that this is a Moufang loop it is thus enough to verify that A is a trilinear alternating form.

Consider $u, v, w \in V$. Then

$$(u, 0)(v, 0) \cdot (w, 0) = (u + v, (u_3 - v_3)(u_1 v_2 - v_2 v_1)) \cdot (w, 0)$$

is equal to $(u + v + w, X)$, where X evaluates to

$$\begin{aligned}
&(u_3 - v_3)(u_1 v_2 - v_2 v_1) + (u_3 + v_3 - w_3)((u_1 + v_1)w_2 - (u_2 + v_2)w_1) \\
&= u_1 u_3 v_2 - u_1 v_2 v_3 - u_2 u_3 v_1 + u_2 v_1 v_3 \\
&\quad + u_1 u_3 w_2 + u_3 v_1 w_2 - u_2 u_3 w_1 - u_3 v_2 w_1 \\
&\quad + u_1 v_3 w_2 + v_1 v_3 w_2 - u_2 v_3 w_1 - v_2 v_3 w_1 \\
&\quad - u_1 w_2 w_3 - v_1 w_2 w_3 + u_2 w_1 w_3 + v_2 w_1 w_3.
\end{aligned}$$

Similarly,

$$(u, 0) \cdot (v, 0)(w, 0) = (u, 0)(v + w, (v_3 - w_3)(v_1 w_2 - v_2 w_1))$$

yields $(u + v + w, Y)$, where Y is equal to

$$\begin{aligned}
&(v_3 - w_3)(v_1 w_2 - v_2 w_1)) + (u_3 - v_3 - w_3)(u_1(v_2 + w_2) - u_2(v_1 + w_1)) \\
&= v_1 v_3 w_2 - v_1 w_2 w_3 - v_2 v_3 w_1 + v_2 w_1 w_3 \\
&\quad + u_1 u_3 v_2 + u_1 u_3 w_2 - u_2 u_3 v_1 - u_2 u_3 w_1 \\
&\quad - u_1 v_2 v_3 - u_1 v_3 w_2 + u_2 v_1 v_3 + u_2 v_3 w_1 \\
&\quad - u_1 v_2 w_3 - u_1 w_2 w_3 + u_2 v_1 w_3 + u_2 v_1 w_3.
\end{aligned}$$

Since $A(u, v, w) = X - Y$, the value of $A(u, v, w)$ is equal to

$$u_3 v_1 w_2 - u_3 v_2 w_1 + 2u_1 v_3 w_2 - 2u_2 v_3 w_1 - u_1 v_2 w_3 + u_2 v_1 w_3.$$

In characteristic 3 this coincides with $\det(u, v, w)$. The determinant is, of course, a trilinear alternating form.

Note that $(u, a)(u, a) = (-u, -a)$ and that $(u, a)(-u, -a) = (0, 0)$ for all $(u, a) \in V \times F$. The neutral element of the loop Q is equal to $(0, 0)$. Note that if the neutral element is also denoted by 1, then $x^3 = 1$ for each $x \in Q$.

When referring to a *commutative Moufang loop* it is quite common to use an abbreviation CML. A CML Q in which $x^3 = 1$ holds for each $x \in Q$ is said to be a CML of *exponent three*.

A central endomorphism. *Let Q be a CML. The mapping $x \mapsto x^3$ is an endomorphism of Q. Put $Z = \{x^3;\ x \in Q\}$. Then $Z \leq Z(Q)$. The loop Q/Z is of exponent three.*

Proof. Since Q is diassociative, $\langle x, y \rangle$ is a commutative group for any choice of $x, y \in Q$. Therefore $(xy)^n = x^n y^n$ for any $n \geq 1$. The only fact to prove thus is that $x^3 \in Z(Q)$. Because Q is commutative it suffices to show that $x^3 \in N(Q)$. Since Q is Moufang, T_x is an automorphism with (the right) companion x^3. This implies that $x^3 \in N(Q)$ if and only if $R_x^{-1} L_x \in \mathrm{Aut}(Q)$. If Q is commutative, then $R_x^{-1} L_x$ is equal to id_Q, which certainly is an automorphism of Q. □

Structure of CML. A CML Q has a *torsion part*, which is the subloop of all elements of finite order. A CML that is equal to its torsion part is said to be a *torsion CML*. A torsion CML that contains no element of order three has to be an abelian group since each element of such a CML can be expressed as a cube. From this it is not difficult to prove that each torsion CML Q may be uniquely expressed as $G \times S$, where G is an abelian group that contains no element of order three and S is the subloop of all elements that are of order 3^k for some $k \geq 0$.

A more difficult proof shows that *each finitely generated CML is nilpotent*.

CML of exponent three and HTS. The abbreviation HTS refers to a *Hall Triple System*. This is an STS with the property that each three elements that do not form a block are contained in an affine subsystem of order 9.

Let V be a vector space over $\mathbb{F}_3$. The operation $*$ of the affine STS upon V is given by $x * y = -x - y$. This implies

$$x * (y * z) = x * (-y - z) = -x + y + z = (-x - y) * (-x - z) = (x * y) * (x * z).$$

The operation of HTS is thus (self)*distributive*.

To prove the converse, consider elements x, y and z of a distributive STS quasigroup $(Q, *)$. Denote z by $[0,0]$, y by $[1,0]$ and x by $[0,1]$. Set

$$\begin{array}{lll} [2,0] = [0,0] * [1,0], & [0,2] = [0,0] * [0,1], & [1,1] = [0,2] * [2,0], \\ [2,2] = [0,0] * [1,1], & [1,2] = [1,0] * [1,1], & [2,1] = [0,1] * [1,1]. \end{array}$$

Ensuing additions are performed modulo 3. If $[a,b] * [c,d] = [e,f]$ and $e = -a - c$ and $f = -b - d$, then $[a,b] * [e,f] = [c,d]$ and $c = -a - e$ and $d = -b - f$. For $a, b, c, d \in \mathbb{F}_3$ the equation $[a,b] * [c,d] = [-a - c, b - d]$ thus holds for the six affine lines of $V = F \times F$. The six missing lines are those that pass through $(2,2)$, with the exception of $\{(0,0),(1,1),(2,2)\}$, and the lines $\{(0,0),(2,1),(1,2)\}$, $\{(0,2),(1,0),(2,1)\}$ and $\{(2,0),(0,1),(1,2)\}$. The distributivity implies

$$\begin{aligned} &[0,0] * [1,1] = [0,0] * ([2,0] * [0,2]]) = ([0,0] * [2,0]) * ([0,0] * [0,2]), \\ &[1,0] * [0,1] = ([0,0] * [2,0]) * ([0,0] * [0,2]) = [0,0] * [1,1] = [2,2], \\ &[2,1] * [1,2] = [1,1] * ([0,1] * [1,0]) = [1,1] * [2,2] = [0,0], \\ &[1,0] * [2,1] = [1,0] * ([0,0] * [1,2]) = [2,0] * [1,1] = [0,2], \text{ and} \\ &[2,0] * [2,1] = [0,0] * ([1,0] * [1,2]) = [0,0] * [1,1] = [2,2]. \end{aligned}$$

Equalities $[0,1] * [1,2] = [2,0]$ and $[0,2] * [1,2] = [2,2]$ may be obtained by a mirror argument. The mapping $(a,b) \mapsto [a,b]$ thus yields a surjective homomorphism of $(V, *)$ upon the subsystem of Q generated by x, y and z. If the homomorphism is not injective, then either $\{x,y,z\}$ is a block, or $x = y = z$. This proves that distributive STS systems are exactly the HTS systems.

To get the connection to CMLs fix an element a of an STS quasigroup Q. Then $xy = x/a*a\backslash y = (x*a)*(a*y)$ is a commutative loop operation with $a = a*a$ being the unit. Note that $xx = x * a$ and that $x \cdot xx = xx \cdot x = x^3 = a$. If the operation star is distributive, then $xy = a * (x * y)$. In such a case $xy \cdot x = (a * (x * y)) \cdot x = (x*y)*(x*a) = x*(a*y)$. Therefore $(x \cdot yz)x = x*(a*(yz)) = x*(y*z)$. Furthermore, $xy \cdot zx = (a*(x*y)) \cdot (a*(x*z)) = (x*y)*(x*z) = x*(y*z)$. This verifies that $(Q, \cdot)$ is a CML of exponent three. Note that $(xy)^{-1} = (xy)^2 = a*(xy) = a*(a*(x*y)) = x*y$. This can be used to get a converse construction.

Indeed, if Q is a CML of exponent three, then $x * y = (xy)^2$ is an idempotent commutative quasigroup that is semisymmetric since $x * (y * x) = x * (xy)^2 = x^2(xy) = y$. Hence $(Q, *)$ is an STS quasigroup. To prove the distributivity note that $x*(y*z) = x*(yz)^2 = x^2(yz) = x(yz)x = xy \cdot zx = (xy)^2 * (xz)^2 = (x*y)*(x*z)$.

Let us mention in passing that it is easy to verify that the identity $x^2 \cdot yz = xy \cdot xz$ in fact describes the variety of CML loops.

We may thus conclude by the following.

Characterization of HTS with CML involved. *An STS system given by an idempotent operation $*$ is an HTS if and only if the operation $*$ is distributive. In such a case for any $a \in Q$ the operation $xy = a * (x * y)$ is a CML of exponent three, and $x * y = (xy)^2$ for all $x, y \in Q$. If $(Q, \cdot)$ is a CML of exponent three, then $x * y = (xy)^2$ provides Q with a structure of HTS.*

Code loops. Their associators and commutators. A Moufang loop Q is said to be a *code loop* if it contains a two-element central subloop Z such that Q/Z is a finite elementary abelian 2-group.

The connection of code loops to error correcting codes (more precisely to double even binary codes) will be explained later. Let us now record several facts that may be derived from results obtained earlier. The factor loop Q/Z may be identified with a vector space V over $F = \{0, 1\}$.

The loop Q is of nilpotence class two. An isomorphic copy of Q may be thus constructed upon $V \times F$, with an operation $(u, a)(v, b) = (u + v, \vartheta(u, v) + a + b)$, where $\vartheta \colon V \times V \to F$ fulfils $\vartheta(u, 0) = \vartheta(0, u) = 0$, for every $u \in V$.

There exist mappings $C \colon V \times V \to F$ and $A \colon V \times V \times V \to F$ such that the isomorphic copy of Q fulfils

$$[(u, a), (v, b)] = (0, C(u, v)) \qquad \text{and} \qquad [(u, a), (v, b), (w, c)] = (0, A(u, v, w)).$$

Note that since the element $1 \in F$ fulfils $-1 = 1$, the signs (or inverses) relating to $A(u, v, w)$ bear no effect. This means that A may be regarded as a trilinear alternating (and thus symmetric) form $V \to F$.

The loop Q satisfies the law $x(y \cdot zx) = (xy \cdot z)x$ since Q is an extra loop. Thus

$$\begin{aligned} x(y \cdot zx) &= \big((y \cdot zx)x\big)[x, y \cdot zx] = \big((y \cdot xz)x\big)[x, z][x, y \cdot zx] \\ &= \big((yx \cdot z)x\big)[y, x, z][x, z][x, y \cdot zx] \\ &= \big((xy \cdot z)x\big)[y, x][y, x, z][x, z][x, y \cdot zx]. \end{aligned}$$

Hence $[y, x][y, x, z][x, z][x, y \cdot zx] = 1 = [x, y, z][x, y][x, z][x, y \cdot zx]$. Therefore

$$A(u, v, w) = C(u, v) + C(u, w) + C(u, u + v + w)$$

for all $u, v, w \in V$. This may be further simplified after recalling that $[x, y] = x^2y^2(xy)^2$ for all $x, y \in Q$. The latter equality holds because of the diassociativity and because x^2 is central and $x^3 = x^{-1}$. It follows by $[x, y] = x^3y^3xy = x^2(xyxy)y^2$.

If $z \in Z$, then $(xz)^2 = x^2$. Hence there exists a mapping $P \colon V \to Z$ such that $P(xZ) = 0$ if $x \in Q$ is of order 1 or 2, and $P(xZ) = 1$ if x is of order 4. The identity $[x, y] = x^2y^2(xy)^2$ means that

$$C(u, v) = P(u) + P(v) + P(u + v) \quad \text{for all } u, v \in V.$$

This implies that

$$C(u, u + v) = P(u) + P(u + v) + P(v) = C(u, v).$$

Therefore $C(u, u + v + w) = C(u, v + w)$ and

$$\begin{aligned} A(u, v, w) &= C(u, v) + C(u, w) + C(u, v + w) \\ &= P(u) + P(v) + P(w) + P(u{+}v) + P(u{+}w) + P(v{+}w) + P(u{+}v{+}w), \end{aligned}$$

for all $u, v, w \in V$. The commutator and associator of Q are thus fully determined by the mapping P.

Combinatorial degree. Let V be a vector space over the 2-element field $F = \{0,1\}$, and let $P\colon V \to F$ be such that $P(0) = 0$. The mapping P is said to be of *combinatorial degree* 0 if $P(v) = 0$ for all $v \in V$. The mapping P is said to be of *combinatorial degree* $k \geq 1$ if

$$(u_1, \ldots, u_k) \mapsto \sum_{1 \leq j \leq k} \sum_{1 \leq i_1 < \cdots < i_j \leq k} P(u_{i_1}) + \cdots + P(u_{i_k})$$

is a k-linear map, and P is not of combinatorial degree $k-1$. Note that P is of combinatorial degree 1 if and only if it it is a nontrivial linear form, and of combinatorial degree 2 if and only if it is a quadratic form that is not a linear form.

We have seen that squares of a code loop yield a mapping of a combinatorial degree 3. For the converse direction consider a mapping $P\colon V \to F = \{0,1\}$, $P(0) = 0$, that is of combinatorial degree at most 3. Set $C(u,v) = P(u) + P(v) + P(u+v)$ and $A(u,v,w) = C(u,v) + C(u,w) + C(u,v+w)$, for all $u, v, w \in V$. The mapping A is a symmmetric trilinear form $V \to F$. It is alternating since, e.g., $A(u,v,v) = 2C(u,v) + C(u,2v) = 0$. Our aim now is to prove that each P that is of combinatorial degree at most three, $P(0) = 0$, induces a code loop the structure of which is determined by P uniquely, up to isomorphism.

Code loops from square mappings of combinatorial degree three. Let $P\colon V \to \{0,1\}$, $P(0) = 0$, be of combinatorial degree at most 3. Define C and A as above.

Our aim is to show that there exists a code loop Q such that Q/Z may be identified with V, and P is induced by the square mapping $x \mapsto x^2$. We shall proceed by assuming that Q exists and derive from that a formula for the operation. To prove the existence of Q it will then suffice to verify that the obtained formula really gives a code loop. For that a construction established earlier may be used. That is the construction of a Moufang loop with operation $(u,a)(v,b) = (u+v, q(u,v) + a + b)$, where $q\colon V \times V \to F$ is linear in the second coordinate and quadratic in the first coordinate, with $q(u+v,v) = q(u,v) + q(v,v)$ for all $u, v \in V$.

Let $b_1, \ldots, b_n$ be a basis of V, and let $e_1, \ldots, e_n \in Q$ be such that $b_i = e_i Z$ for each $i \in \{1, \ldots, n\}$. Each element of Q may be uniquely expressed in a *normal form* as

$$(e_{i_1}(e_{i_2}(\cdots(e_{i_{k-1}}e_{i_k}))))z, \text{ where } 1 \leq i_1 < \cdots < i_k \leq n \text{ and } z \in Z.$$

This follows from the fact that $e_{i_1}(e_{i_2}(\cdots e_{i_k}))$ projects upon $\sum \lambda_j b_j$, where $\lambda_j = 1$ if j occurs in the sequence $i_1, \ldots, i_k$, while otherwise $\lambda_j = 0$. We shall identify Q with $V \times F$ in such a way that

$$(e_{i_1}(e_{i_2}(\cdots e_{i_k})))z \mapsto \begin{cases} (\sum \lambda_j b_j, 0) & \text{if } z = 1, \\ (\sum \lambda_j b_j, 1) & \text{if } z \neq 1. \end{cases}$$

Assume $k \geq 1$, put $j = i_1$ and $y = e_{i_2}(\cdots(e_{i_{k-1}}e_{i_k}))$. If $i \in \{1, \ldots, k\}$, then

$$e_i(e_j y) = \begin{cases} e_i(e_{i_1}(e_{i_2}(\cdots(e_{i_{k-1}}e_{i_k})))) \text{ if } i < j, \\ (e_{i_2}(\cdots(e_{i_{k-1}}e_{i_k})))\, e_j^2 \text{ if } i = j, \text{ and} \\ (e_i e_j)y\, [e_i, e_j, y] = (e_j e_i)y\, [e_i, e_j][e_i, e_j, y] = e_j(e_i y)\, [e_i, e_j] \text{ if } i > j. \end{cases}$$

The last equality follows from $(e_j e_i)y = e_j(e_i y)\, [e_j, e_i, y]$ and $[e_j, e_i, y] = [e_i, e_j, y]$.

To multiply $x = e_{i_1}(e_{i_2}(\cdots(e_{i_{k-1}}e_{i_k})))$ by e_i from the left thus means to shift e_i to the right until it reaches e_{i_ℓ}, where $i \leq i_\ell$. During its travel to the right e_i produces all $[e_i, e_{i_j}]$ where $i_j < i$, and also e_i^2 if $i = i_\ell$. In the latter case $e_i = e_{i_\ell}$ is

removed from the list. Writing this in the language of $V \times F$ gives

$$(b_i, 0)\left(\sum_j \lambda_j b_j, 0\right) = \left(\sum_j (\lambda_j + \delta_{ij}) b_j,\ \lambda_i P(e_i) + \sum_{i>j} \lambda_j C(e_i, e_j)\right),$$

where $\delta_{ij} \in \{0, 1\}$ is equal to 1 if and only if $i = j$.

For the case of a general product note that $e_\ell x \cdot y = (e_\ell \cdot xy)[e_\ell, x, y]$. If $e_\ell x$ is in a normal form, y is in a normal form, and the transformation of xy into a normal form has been already performed, the final step of transformation of $e_\ell x \cdot y$ into a normal form rests in putting $[e_\ell, x, y]$ together with all $[e_\ell, e_j]$ such that e_j occurs in the normal form of y and $j < \ell$. If e_ℓ occurs in the normal form of y, then e_ℓ is removed from the normal form, while e_ℓ^2 contributes to the element of Z that appears as the rightmost element of the normal form. To see that the latter is true note that while e_ℓ interacts with the normal form of xy, the interaction is restricted to the part on the left in which there occur indices $\leq \ell$. This part of the normal form of xy coincides with the corresponding left part of y since ℓ is the smallest index occuring in x.

This gives a recursive procedure for a transformation into a normal norm of any two products. Let the projection of $e_\ell x$ be $u = \sum \lambda_i b_i$ and suppose that y projects to $v = \sum \nu_i b_i$. The mapping A is trilinear. The contribution of associators thus amounts to the sum of all $A(\lambda_i b_i, \lambda_j b_j, \nu_k b_k)$, where $i < j$. The product of $(u, 0)$ and $(v, 0)$ is thus equal to $(u + v, q(u, v))$, where

$$q(u, v) = \sum_k \nu_k \left(\lambda_k P(b_k) + \sum_{i>k} \lambda_i C(b_i, b_k) + \sum_{i<j} \lambda_i \lambda_j A(b_i, b_j, b_k)\right).$$

The mapping q clearly is linear in the second variable. Sums of quadratic forms are quadratic forms. Hence to prove that q is quadratic in the first variable it suffices to verify that the mapping

$$q_k(u) = \lambda_k P(b_k) + \sum_{i>k} \lambda_i C(b_i, b_k) + \sum_{i<j} \lambda_i \lambda_j A(b_i, b_j, b_k)$$

is quadratic for each $k \in \{1, \ldots, n\}$. Let $u = \sum \lambda_i b_i$ and $v = \sum \nu_i b_i$. The contributions of P and C in $q_k(u) + q_k(v) + q_k(u + v)$ amount to

$$(\lambda_k + \nu_k + (\lambda_k + \nu_k))P(b_k) + \sum_{i>k} ((\lambda_i + \nu_i + (\lambda_i + \nu_i))C(b_i, b_k).$$

This vanishes. Since $\lambda_i \lambda_j + \nu_i \nu_j + (\lambda_i + \nu_i)(\lambda_j + \nu_j)$ yields $\lambda_i \nu_j + \lambda_j \nu_i$ we see that

$$q_k(u) + q_k(v) + q_k(u + v) = \sum_{i,j} \lambda_i \nu_j A(b_i, b_j, b_k)$$

is bilinear. It remains to verify that $q(u + v, v) = q(u, v) + q(v, v)$. To see this observe first that $q(u, v)$ may be also expressed as

$$\sum_k \nu_k \left(\lambda_k P(b_k) + \sum_{i>k} \lambda_i C(b_i, b_k)\right) + \sum_{\{i,j,k\}} (\lambda_i \lambda_j \nu_k + \lambda_i \nu_j \lambda_k + \nu_i \lambda_j \lambda_k) A(b_i, b_j, b_k).$$

The sum upon the right runs over all 3-element subsets of $\{1, \ldots, n\}$. The formula is independent of the ordering of the subset. To see the connection to the original expression of $q(u, v)$, assume $i < j < k$ and note that the original formula carries

$$\nu_k \lambda_i \lambda_j A(b_i, b_j, b_k) + \nu_j \lambda_i \lambda_k A(b_i, b_k, b_j) + \nu_i \lambda_j \lambda_k A(b_j, b_k, b_i)$$

and that these are all occurences of $A(b_{\sigma(i)}, b_{\sigma(j)}, b_{\sigma(k)})$ in the formula, where σ is a permutation of $\{i, j, k\}$.

Since $(\lambda_k+\nu_k)P(b_k)=\lambda_kP(b_k)+\nu_kP(b_k)$ and $(\lambda_i+\nu_i)C(b_i,b_k)=\lambda_iC(b_i,b_k)+\nu_iC(b_i,b_k)$ the proof of $q(u+v,v)=q(u,v)+q(v,v)$ requires verification only for the coefficients of $A(b_i,b_j,b_k)$. However,

$$(\lambda_i+\nu_i)(\lambda_j+\nu_j)\nu_k+(\lambda_i+\nu_i)\nu_j(\lambda_k+\nu_k)+\nu_i(\lambda_j+\nu_j)(\lambda_k+\nu_k)$$

evaluates to

$$\lambda_i\lambda_j\nu_k+\lambda_i\nu_j\lambda_k+\nu_i\lambda_j\lambda_k+3\nu_i\nu_j\nu_k$$

which is exactly the aggregated contribution of $q(u,v)+q(v,v)$.

This verifies that the procedure yields a code loop. If at the beginning there had been a code loop Q the squares of which induce P, the constructed loop is isomorphic to Q since $q(u,v)$ expresses products of elements in a normal form. A normal form depends upon the choice of basis. The formula for $q(u,v)$ thus provides loops isomorphic to Q for any choice of basis $b_1,\dots,b_n$.

Consider now a situation when at the beginning there was only a mapping P of combinatorial degree at most three, $P(0)=0$. By means of $q(u,v)$ we have constructed a code loop in which squaring is given by $\tilde{P}(u)=q(u,u)$. The question is whether $\tilde{P}=P$. If this is true, then by the argument above the formula for $q(u,v)$ provides a code loop the isomorphism type of which does not dependent upon the choice of basis.

The proof of $\tilde{P}=P$ is divided into two steps. Assume $1\le i<j<k\le n$. We have

$$\begin{aligned}
(b_k,0)(b_k,0)&=(0,P(b_k)),\\
(b_i+b_k,0)^2&=(0,P(b_i)+P(b_j)+C(b_k,b_i))=(0,P(b_i+b_k)),\ \text{and}\\
(b_i+b_j+b_k,0)^2&=(0,P(b_i)+P(b_j)+P(b_k)\\
&\quad+C(b_j,b_i)+C(b_k,b_j)+C(b_k,b_i)+A(b_i,b_j,b_k))\\
&=(0,P(b_i)+P(b_j)+P(b_k)+P(b_i+b_j)+P(b_j+b_k)\\
&\quad+P(b_i+b_k)+A(b_i,b_j,b_k))\\
&=(0,P(b_i+b_j+b_k)).
\end{aligned}$$

This shows that $\tilde{P}$ and P agree at all values b_i, b_i+b_j and $b_i+b_j+b_k$. Hence they agree everywhere, as will be proved now.

Values that determine the square mapping completely. *Let $P\colon V\to\{0,1\}$, $P(0)=0$, be a mapping of combinatorial degree at most three. Let $b_1,\dots,b_n$ be a basis of V. Then P is completely determined by all of the values $P(b_i)$, $P(b_i+b_j)$ and $P(b_i+b_j+b_k)$, where $i,j,k\in\{1,\dots,n\}$.*

Proof. For each $u=\sum\lambda_iu_i\in V$ denote by $|u|$ the number of $i\in\{1,\dots,n\}$ such that $\lambda_i=1$. Call $|u|$ the *weight* of u. The value of $P(u)$ is known if $|u|\le3$. We shall show by induction that each $P(u)$ may be expressed as a sum of $P(w)$, where $|w|\le3$. To do so express u as $v+e_i+e_j+e_k$, where $|u|-3=|v|\ge1$. Then $A(v+e_i,e_j,e_k)=A(v,e_j,e_k)+A(e_i,e_j,e_k)$. The expression of $A(v+e_i,e_j,e_k)$ by means of P is a sum of $P(u)$ and of P-values for vectors of weight $<|u|$. The expressions of $A(v,e_j,e_k)$ and $A(e_i,e_j,e_k)$ also consists of sums of $P(w)$, where $|w|<|u|$. Hence $P(u)$ may be expressed as such a sum too, and that makes the induction applicable. □

Existence and uniqueness of code loops. *Let V be a vector space over $F=\{0,1\}$ with a basis $b_1,\dots,b_n$. For each mapping $P\colon V\to F$, $P(0)=0$, that is of combinatorial degree at most three there exists, up to isomorphism, a unique code loop $(Q,\cdot,1)$ with a central subloop Z, $|Z|=2$, where V is identified with Q/Z in such a way that $P(xZ)=0$ if $x^2=1$ and $P(xZ)=1$ otherwise. Such a loop is*

always isomorphic to a loop $V[P]$ that is defined upon $V \times F$ in such a way that if $u = \sum \lambda_i b_i$, $v = \sum \nu_i b_i$ and $a, b \in F$, then $(u, a) \cdot (v, b) = (u + v, a + b + c)$, where c is equal to

$$\sum_k \nu_k \left(\lambda_k P(b_k) + \sum_{i>k} \lambda_i C(b_i, b_k) \right) + \sum_{\{i,j,k\}} (\lambda_i \lambda_j \nu_k + \lambda_i \nu_j \lambda_k + \nu_i \lambda_j \lambda_k) A(b_i, b_j, b_k),$$

with $C(x, y) = P(x)+P(y)+P(x+y)$ and $A(x, y, z) = C(x, z)+C(y, z)+C(x+y, z)$ for all $x, y, z \in V$.

If $P_i \colon V \to F$, $P_i(0) = 0$, $i \in \{1, 2\}$ are two mappings of combinatorial degree three, then $V[P_1] \cong V[P_2]$ if and only if there exists a linear automorphism $\alpha \in \mathrm{Aut}(V)$ such that $P_2(v) = P_1(\alpha(v))$ for each $v \in V$.

Proof. Only the part about the isomorphism of $V[P_1]$ and $V[P_2]$ requires a proof. Assume first the existence of α and extend it to a permutation $\bar{\alpha}$ of $V \times F$, $\bar{\alpha}(u, a) = (\alpha(u), a)$. The mapping $\bar{\alpha}$ induces a loop Q upon $V \times F$ such that $\bar{\alpha} \colon Q \cong V[P_1]$. The square of (u, a) in Q is equal to $\bar{\alpha}^{-1}((\bar{\alpha}(u, a))^2) = \bar{\alpha}^{-1}((\alpha(u), a)^2) = \bar{\alpha}^{-1}(0, P_1(\alpha(u))) = \bar{\alpha}^{-1}(0, P_2(u)) = (0, P_2(u))$. Therefore $Q \cong P_2[V]$. Since Q is defined in such a way that $Q \cong V[P_1]$, there must be $V[P_1] \cong V[P_2]$.

For the converse direction suppose that $\psi \colon V[P_2] \cong V[P_1]$. Since both P_1 and P_2 are of combinatorial degree three, the central associator elements of both $V[P_1]$ and $V[P_2]$ are equal to $(0, 0)$ and $(0, 1)$. Therefore ψ induces a linear automorphism α such that for each $(u, a) \in V \times F$ there exists $b \in F$ such that $\psi(u, a) = (\alpha(u), b)$. Hence $(0, P_2(u)) = \psi((u, a)(u, a)) = (\alpha(u), b)(\alpha(u), b) = (0, P_1\alpha(u))$. □

Connection to error correcting codes. A *binary linear code* D is any vector subspace of F^n, $F = \{0, 1\}$, $n \geq 1$. The term *code* is being used when $\min\{|u|; u \in D, u \neq 0\}$ is relatively large if compared to $\dim(D)$ and n. A binary linear code D is called *doubly even* if 4 divides $|u|$ for each $u \in D$. An example of doubly even code is the extended binary Golay code of length $n = 24$.

Let D be a doubly even code. For $u \in D$ set $P(u) = 0$ if 8 divides $|u|$, and $P(u) = 1$ if $|u| \equiv 4 \bmod 8$. If $u, v \in D$, set $C(u, v) = 0$ if $|u \cap v|$ is divisible by 4. Otherwise set $C(u, v) = 1$. (If $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$, then $u \cap v = (u_1 v_1, \ldots, u_n v_n)$.)

Since $|u + v| = |u| + |v| - 2|u \cap v|$ we have $4P(u + v) \equiv 4P(u) + 4P(v) - 4|u \cap v|/2 \bmod 8$. Hence $P(u + v) \equiv P(u) + P(v) + |u \cap v|/2 \bmod 2$. Therefore $C(u, v) = P(u) + P(v) + P(u + v)$.

Since $|(u + v) \cap w| = |(u \cap w)| + |(v \cap w)| - 2|u \cap v \cap w|$ there has to be

$$2C(u + v, w) \equiv 2C(u, w) + 2C(v, w) - 2|u \cap v \cap w| \bmod 4.$$

Put $A(u, v, w) = 0$ if $|u \cap v \cap w|$ is even. Otherwise set $A(u, v, w) = 1$. The congruence above shows that

$$A(u, v, w) \equiv C(u + v, w) + C(u, w) + C(v, w) \bmod 2$$

for all $u, v, w \in V$. It is clear that $A(u, u, v) = 0$. The equality $A(u + v, w, z) = A(u, w, z) + A(v, w, z)$ follows from $(u + v) \cap w \cap z = u \cap w \cap z + v \cap w \cap z$ since $A(u, v, w)$ gives the parity of $|u \cap v \cap w|$.

The mapping P therefore is of combinatorial degree at most 3. As such it induces a code loop upon $D \times F$. It may be proved that for each code loop Q there exists a code D that induces a loop isomorphic to Q.

The loop induced by the extended binary Golay code is known as *Parker loop*. The Parker loop may be used as a departing point of the construction of the Monster (or Friendly Giant), the largest sporadic finite simple group.