POWER-ASSOCIATIVE, CONJUGACY CLOSED LOOPS

MICHAEL K. KINYON AND KENNETH KUNEN*

Abstract. We study conjugacy closed loops (CC-loops) and power-associative CC-loops (PACC-loops). If Q is a PACC-loop with nucleus N, then Q/N is an abelian group of exponent 12; if in addition Q is finite, then $|Q|$ is divisible by 16 or by 27. There are eight nonassociative PACC-loops of order 16, three of which are not extra loops. There are eight nonassociative PACC-loops of order 27, four of which have the automorphic inverse property.

We also study some special elements in loops, such as Moufang elements, weak inverse property (WIP) elements, and extra elements. In a CC-loop, the set of WIP and the set of extra elements are normal subloops. For each c in a PACC-loop, c^3 is WIP, c^6 is extra, and $c^{12} \in N$.

1. Introduction

A loop is *conjugacy closed* (a *CC-loop*) iff it satisfies the equations:

$$xy \cdot z = xz \cdot (z\backslash(yz)) \quad \text{(RCC)} \qquad\qquad z \cdot yx = ((zy)/z) \cdot zx \quad \text{(LCC)}$$

This definition follows Goodaire and Robinson [14, 15]; CC-loops were earlier introduced independently, with different terminology, by Сойкис [23]. Further discussion can be found in [8, 9, 17, 18]. The literature is not uniform as to which of these two equations is left (LCC) and which is right (RCC). With our choice here, also followed in [10, 21], LCC is equivalent to saying that the set of *left* multiplication maps is closed under conjugation. In [17, 18], the equation labels LCC and RCC were arranged in the opposite order.

In 1982, Goodaire and Robinson [14] showed that the nucleus $N(Q)$ of a CC-loop Q is a normal subloop. A fundamental result in the theory of CC-loops was proved in 1991:

Theorem 1.1 (Басараб [2])**.** *Let Q be a CC-loop with nucleus $N = N(Q)$. Then Q/N is an abelian group.*

This was conjectured in [14], but Басараб was apparently unaware of the conjecture, since he was following the terminology of Сойкис. Because of the differences in terminology, Theorem 1.1 was not widely known until recently. Proofs in English of Theorem 1.1 can be found in [8, 17].

Date: January 13, 2006.

2000 *Mathematics Subject Classification.* 20N05.

Key words and phrases. conjugacy closed loop, power-associative, extra loop.

*Partially supported by NSF Grants DMS-0097881 and DMS-0456653.

The CC-loops which are also *diassociative* (that is every $\langle x, y\rangle$ is a group) are precisely the *extra loops* of Fenyves [12, 13]. For these, a detailed structure theory was described in [16]. The current paper gives a structure theory for those CC-loops which are only power-associative.

Definition 1.2. *For any loop Q:*

1. *For $c \in Q$, define c^ρ and c^λ by: $cc^\rho = c^\lambda c = 1$.*
2. *$c \in Q$ is* power-associative *iff the subloop $\langle c\rangle$ is a group. Q is* power-associative *iff every element is power-associative. A* PACC-loop *is a power-associative CC-loop.*

The two parts of this definition are related by:

Lemma 1.3 ([18])**.** *Let c be an element of a CC-loop Q. Then*

$$c \text{ is power associative} \qquad \text{iff} \qquad c^\rho = c^\lambda \qquad \text{iff} \qquad cc^2 = c^2c$$

If Q is a finite nonassociative extra loop, then $16 \mid |Q|$ (see [16, 17]), and there are exactly five nonassociative extra loops of order 16 (see Chein [5], p. 49). We shall show here (Theorem 6.4) that if Q is a finite nonassociative PACC-loop, then $16 \mid |Q|$ or $27 \mid |Q|$. Furthermore (see §8), there are exactly eight nonassociative PACC-loops of order 16 (including the five extra loops), and (see §9) there are exactly eight nonassociative PACC-loops of order 27. In §7, we describe a method of loop extension which will be useful in constructing the loops in §§8,9. In §5, we prove some results about PACC-loops for which $Q/N(Q)$ is small; these results will be useful for describing the PACC-loops of small orders.

In §§3,4, we discuss some special kinds of elements in general CC-loops. Besides the power-associative elements defined above, there are Moufang and pseudoMoufang elements, extra elements, and WIP (weak inverse property) elements. A loop is an extra loop iff all its elements are extra elements; likewise for Moufang and WIP. These special elements help us prove some facts about PACC-loops. For example (Theorem 4.20), if c is in a PACC-loop Q, then $c^{12} \in N(Q)$; and this is proved by showing that c^3 is a WIP element and c^6 is an extra element.

We shall begin in §2 be describing some basic facts about inner mappings, autotopisms, etc.

Our investigations were aided by the automated reasoning tool OTTER [20], and the finite model builder Mace4 [19], both developed by McCune. We would also like to thank the referee for many useful suggestions.

2. Inner Mappings, Commutators, and Associators

As usual in a loop Q, we define the right and left multiplications by $xy = xR_y = yL_x$. These permutations define a number of important subgroups of $\mathrm{Sym}(Q)$:

$$\begin{array}{lll} \mathrm{Mlt}(Q) := \langle R_x, L_x : x \in Q\rangle & \mathrm{RMlt}(Q) := \langle R_x : x \in Q\rangle & \mathrm{LMlt}(Q) := \langle L_x : x \in Q\rangle \\ \mathrm{Inn}(Q) := (\mathrm{Mlt}(Q))_1 & \mathrm{RInn}(Q) := (\mathrm{RMlt}(Q))_1 & \mathrm{LInn}(Q) := (\mathrm{LMlt}(Q))_1 \end{array}$$

$\mathrm{Mlt}(Q)$ is called the *multiplication group* of a loop Q; it is generated by all the multiplications. Then the *inner mapping group* $\mathrm{Inn}(Q)$ is the stabilizer in $\mathrm{Mlt}(Q)$ of the identity element 1. By using only right or only left multiplications, we get the *right* and *left multiplication groups* and the *right* and *left inner mapping groups*.

For $x, y, z \in Q$, define

$$R(x,y) := R_x R_y R_{xy}^{-1} \qquad L(x,y) := L_x L_y L_{yx}^{-1}$$
$$T_x := R_x L_x^{-1}$$

These are the standard generators of the inner mapping groups [3, 4]:

$$\mathrm{Inn}(Q) = \langle R(x,y), L(x,y), T_x : x, y \in Q \rangle$$
$$\mathrm{RInn}(Q) = \langle R(x,y) : x \in Q \rangle \qquad \mathrm{LInn}(Q) = \langle L(x,y) : x \in Q \rangle$$

Also note that a subloop of Q is normal if and only if it is invariant under the action of $\mathrm{Inn}(Q)$ [4].

Lemma 2.1. *Let Q be a loop with nucleus $N = N(Q)$ such that $N \trianglelefteq Q$ and Q/N is an abelian group. If M is a subloop of Q satisfying $N \le M$, then $M \trianglelefteq Q$.*

Proof. For each $x \in M$, $\varphi \in \mathrm{Inn}(Q)$, there exists $n \in N$ such that $(x)\varphi = xn \in M$. Thus $\mathrm{Inn}(Q)$ leaves M invariant, and so M is normal. □

An *autotopism* of a loop Q is a triple of permutations (α, β, γ) such that $x\alpha \cdot y\beta = (xy)\gamma$ for all $x, y \in Q$. The autotopisms form a subgroup of $\mathrm{Sym}(Q)^3$. Defining

$$\mathcal{R}(z) := (R_z, T_z, R_z) \qquad \mathcal{L}(z) := (T_z^{-1}, L_z, L_z) \quad ,$$

we see that (RCC) and (LCC) are equivalent, respectively, to the assertions that each $\mathcal{R}(z)$ and each $\mathcal{L}(z)$ is an autotopism. In any loop, if (α, β, α) or (β, α, α) is an autotopism and $(1)\alpha = 1$, then $\beta = \alpha$ and α is an automorphism. Applying this in a CC-loop, where $\mathcal{R}(x)\mathcal{R}(y)\mathcal{R}(xy)^{-1}$ and $\mathcal{L}(x)\mathcal{L}(y)\mathcal{L}(yx)^{-1}$ are autotopisms, we get the following lemma, the parts of which are from [14] and [8], respectively.

Lemma 2.2. *For x, y in a CC-loop Q,*

1. *$R(x,y)$ and $L(x,y)$ are automorphisms of Q.*
2. *$R(x,y) = T_x T_y T_{xy}^{-1}$ and $L(x,y) = T_x^{-1} T_y^{-1} T_{yx}$, so that $\mathrm{Inn}(Q)$ is generated by $\{T_x : x \in Q\}$.*

Definition 2.3. *Define the* commutator $[x,y]$ *and the* associator (x,y,z) *by:*

$$xy = yx \cdot [x,y] \qquad xy \cdot z = (x \cdot yz) \cdot (x,y,z) \quad .$$

The associator subloop *is $A(Q) := \langle (x,y,z) : x,y,z \in Q \rangle$.*

By Theorem 1.1, (1) of the following lemma holds for CC-loops.

Lemma 2.4. *In a loop Q with nucleus $N = N(Q)$, the following are equivalent:*

1. *$N \trianglelefteq Q$ and Q/N is commutative.*
2. *Every commutator is contained in N.*

In case these conditions hold, $xT_y = x[x,y]$ for all $x, y \in Q$.

Proof. That (1) implies (2) is clear. If (2) holds, then $y \cdot (x)T_y = xy = yx[x,y]$, so $xT_y = x[x,y]$. Thus, $NT_y \subseteq N$ for all y. Since N is also pointwise fixed by $\mathrm{RInn}(Q)$ and $\mathrm{LInn}(Q)$, we have $N \trianglelefteq Q$, and hence (1). $\square$

$A = A(Q)$ is not in general a normal subloop of Q; if it is normal, then Q/A is defined, and it is clearly a group. The next lemma implies that $A \trianglelefteq Q$ for CC-loops, since $A \leq N(Q)$ by Theorem 1.1.

Lemma 2.5. *Let Q be a loop with associator subloop $A = A(Q)$. If $A \leq N(Q)$, then for all $x, y, z, u \in Q$,*

1. $(x,y,z)T_u = (x,yz,u)^{-1}(y,z,u)^{-1}(x,y,zu)(xy,z,u)$
2. $[(x,y,z),u] = (x,y,z)^{-1}(x,yz,u)^{-1}(y,z,u)^{-1}(x,y,zu)(xy,z,u)$

In particular, $A(Q) \trianglelefteq Q$.

Proof. Compute

$$\begin{aligned}(x \cdot yz)(x,y,z)u = (xy \cdot z)u = xy \cdot zu \cdot (xy,z,u) &= x(y \cdot zu)(x,y,zu)(xy,z,u) \\ &= x(yz \cdot u)(y,z,u)^{-1}(x,y,zu)(xy,z,u) \\ &= (x \cdot yz) \cdot u \cdot (x,yz,u)^{-1}(y,z,u)^{-1}(x,y,zu)(xy,z,u).\end{aligned}$$

Cancel $x \cdot yz$ and then divide both sides on the left by u to obtain (1). (2) follows from (1), using $(x,y,z) \in N$. By (1), $aT_u \in A$ for each generator a of A and each $u \in Q$. It follows that each $AT_u \subseteq A$; to verify this, use $A \leq N(Q)$ and note that $(mn)T_u = mT_u \cdot nT_u$ whenever $m, n, mT_u, nT_u \in N$. Thus, A is normal, since any subloop of $N(Q)$ is pointwise fixed by $\mathrm{RInn}(Q)$ and $\mathrm{LInn}(Q)$. $\square$

Lemma 2.6. *Let Q be a loop with nucleus $N = N(Q)$. If $N \trianglelefteq Q$ and Q/N is a group, then*

1. $(x,y,z) = (ux,vy,wz)$ *for all* $x,y,z \in Q$ *and* $u,v,w \in N$.
2. $A(Q) \leq Z(N)$ *so that* $A(Q)$ *is an abelian group.*
3. $(x^\rho, y, z) = (x^\lambda, y, z)$.

Proof. For (1) and (2), see, for instance, [17], §5. For (3), note that $x^\rho / x^\lambda \in N$. $\square$

In particular, Lemma 2.6 applies to CC-loops by Theorem 1.1.

Lemma 2.7. *In a loop,*

1. RCC *is equivalent to* $(x,y,z) = (x,z,yT_z)$.
2. LCC *is equivalent to* $(x,y,z) = (yT_x^{-1}, x, z)$.

Proof. RCC is equivalent to $xy \cdot z = xz \cdot yT_z$, so (1) is clear from:

$$\begin{aligned} xy \cdot z &= (x \cdot yz) \cdot (x,y,z) \\ xz \cdot yT_z &= (x \cdot (z \cdot yT_z)) \cdot (x,z,yT_z) = (x \cdot yz) \cdot (x,z,yT_z)\end{aligned}$$

(2) is the mirror of (1). $\square$

Lemma 2.8. *A loop Q is a CC-loop iff*

a. *All associators are invariant under permutations of their arguments, and*
b. *All commutators are nuclear.*

Proof. For $\Rightarrow$, (a), which is ([17], Theorem 4.4), follows from Theorem 1.1 and Lemmas 2.6 and 2.7 (since $yT_z = vy$ for some $v \in N$), while (b) follows from Theorem 1.1. For $\Leftarrow$, note that (a), (b), and Lemmas 2.4 and 2.6 yield $(x, y, z) = (x, z, yT_z)$ and $(x, y, z) = (yT_x^{-1}, x, z)$, and then apply Lemma 2.7. $\square$

We shall frequently use Lemmas 2.6 and 2.8 without comment when writing equations with associators. We next collect some further properties of associators in CC-loops.

Lemma 2.9. *In any CC-loop Q:*

1. $(xy, z, u) = (x, z, u)T_y \cdot (y, z, u) = (x, z, u) \cdot (y, z, u)T_x$
2. $[(x, z, u), y] = [(y, z, u), x]$
3. $(x^\rho, z, u)T_x = (x, z, u)^{-1}$
4. $(xy, z, u) = 1$ *iff* $(x, z, u) = (y^\rho, z, u)$
5. *for each $x, y \in Q$, $\{u : (u, x, y) = 1\}$ is a subloop of Q.*

Proof. We know that associators are invariant under permutations of their arguments (Lemma 2.8) and lie in the center of the nucleus (Lemma 2.6). Also, $(xy, z, u) = (yx, z, u)$ because commutators are nuclear. Now, by Lemma 2.5(1),

$$(x, y, z)T_u = (x, yz, u)^{-1}(y, z, u)^{-1}(x, y, zu)(xy, z, u)$$
$$(x, z, y)T_u = (x, zy, u)^{-1}(z, y, u)^{-1}(x, z, yu)(xz, y, u)\,.$$

But these are equal, so

$$(x, y, zu)(xy, z, u) = (x, z, yu)(xz, y, u)\,.$$

Using this and Lemma 2.5(1) again, we get (1):

$$\begin{aligned}(x, z, u)T_y \cdot (y, z, u) =&(x, zu, y)^{-1}(x, z, uy)(xz, u, y) = \\ &(x, zu, y)^{-1}(x, y, uz)(xy, u, z) = (xy, z, u)\,.\end{aligned}$$

(2) follows from Lemma 2.4 and (1). We obtain (3) by taking $y = x^\rho$ in (1). (4) follows from (1) and (3). In (5), note that $\{u : (u, x, y) = 1\} = \{u : uR(x, y) = u\}$, which is a subloop because $R(x, y)$ is an automorphism. $\square$

Lemma 2.10. *For all x, y, z in a CC-loop Q,*

1. $zL(x, y) = z(z, x, y)^{-1}$
2. $zR(x, y) = z(z, x^\lambda, y^\lambda)$
3. $R(x, y)^{-1} = L(x^\lambda, y^\lambda)$, *so that* $\mathrm{RInn}(Q) = \mathrm{LInn}(Q)$.
4. $R(x, y) = R(y, x)$
5. $R(x, y)R(u, v) = R(u, v)R(x, y)$, *so that* $\mathrm{RInn}(Q)$ *is an abelian group.*

Proof. (1) is from ([17], §4). Next, we compute

$$xR(y,z)R_{yz} = xy \cdot z = xR_{yz} \cdot (x,y,z)$$

so that $xR(y,z) = xR_{yz}R_{(x,y,z)}R_{yz}^{-1} = x[(yz \cdot (x,y,z))/(yz)]$. By Lemma 2.9(4), $yz \cdot (x,y,z) = y(x,y,z^\lambda)^{-1}z = (x,y^\lambda,z^\lambda) \cdot yz$, and (2) holds. (3) follows from (1), (2), and Lemma 2.2(1). (4), which is from [17], follows from (3) and Lemma 2.9(1). (5), which is also from [17], follows from (2) and Lemmas 2.2(1) and 2.6(1). ☐

By finding an expression for $L(x,y)$ as a product of right multiplications, Drápal [8] was the first to show that $\mathrm{RInn}(Q) = \mathrm{LInn}(Q)$ for a CC-loop Q. However, the equation in Lemma 2.10(3) relating the generators of the two groups seems to be new.

The following inner mapping was used also in [17, 18]:

$$E_x := R(x,x^\rho) = R_x R_{x^\rho} \quad .$$

The next lemma collects some of its properties:

Lemma 2.11. *For every x,y in a CC-loop Q:*

1. *Each E_x is an automorphism.*
2. *$yE_x = y(y,x^\lambda,x)$.*
3. *$E_x = R(x^\lambda,x) = L(x,x^\lambda)^{-1} = L(x^\rho,x)^{-1} = R_xL_xR_x^{-1}L_x^{-1}$.*
4. *If x is power-associative, then $E_{x^n} = E_x^{n^2}$, $[E_x,L_x] = [E_x,R_x] = I$, and $R_{x^n} = R_x^nE_x^{(n-1)n/2}$, $L_{x^n} = L_x^nE_x^{-(n-1)n/2}$, $R_x^nL_x^m = L_x^mR_x^nE_x^{mn}$.*
5. *If Q is a PACC-loop, then $E_x^6 = I$.*

Proof. (1) and (2) are just specializations of Lemmas 2.2(1) and 2.10(2), respectively. The first two equalities of (3) follow from (2) and Lemma 2.10(1)(2); that is, $yR(x^\lambda,x) = y(y,x,x^\lambda)$ and $yL(x,x^\lambda)^{-1} = y(y,x,x^\lambda)$. The third equality follows from these and Lemma 2.6(3). The remaining equality of (3) is from [18], as is (4). (5) is from [17]. ☐

We conclude this section with the following easy criterion for checking that a subset is a subloop:

Lemma 2.12. *A subset X of a CC-loop Q is a subloop iff X is closed under product and either ρ or λ.*

Proof. By Lemma 2.11, $L_x^{-1} = E_xL_{x^\rho} = L_{x^\lambda}E_x$ and $R_x^{-1} = R_{x^\rho}E_x^{-1} = E_x^{-1}R_{x^\lambda}$. This yields the equations

$$\begin{aligned} x\backslash y &= x^\rho(yx \cdot x^\rho) &&= (x^\lambda y \cdot x^\lambda)x \\ y/x &= x(x^\rho \cdot yx^\rho) &&= (x^\lambda \cdot xy)x^\lambda \end{aligned}$$

which immediately yield the desired result. ☐

3. WIP Elements

The role played by weak inverse property elements in CC-loops was already highlighted in [15, 17]. In this section we elaborate further on that theme.

Definition 3.1. *An element c of a loop Q is a* weak inverse property (WIP) element *iff for all $x \in Q$,*

$$c(xc)^\rho = x^\rho \qquad (cx)^\lambda c = x^\lambda\,. \tag{WIP}$$

Let $W(Q)$ denote the set of all WIP elements of Q.

The two equations defining a WIP element are equivalent in all loops ([17], Lemma 2.18). Also note that $N(Q) \subseteq W(Q)$.

Lemma 3.2. *For an element c of a CC-loop, the following are equivalent; in (ii)–(vii), the variable x is understood to be universally quantified:*

i. c *is a WIP element*

ii.	$x(cx)^\rho = c^\rho$	*iii.*	$(xc)^\lambda x = c^\lambda$
iv.	$c = (c \cdot xE_c)x^\rho$	*v.*	$x = (x \cdot cE_x)c^\rho$
vi.	$(c, x, x^\rho) = (x^\rho, c, c^\rho)$	*vii.*	$(x, c, c^\rho) = (c^\rho, x, x^\rho)$.

Proof. (i) holds iff $x \cdot c(xc)^\rho = 1$, that is, iff $c \cdot [c\backslash(xc)](xc)^\rho = 1$ for all x, using LCC. Replacing x with $(cx)/c$, we have that (i) holds iff $c \cdot x(cx)^\rho = 1$ for all x. Thus $(i) \leftrightarrow (ii)$, and the mirror of this argument yields $(i) \leftrightarrow (iii)$.

Next, (i) holds iff $(xc)^\rho = c\backslash x^\rho$; that is, $1 = xc \cdot (c\backslash x^\rho)$. Multiplying on the left by c and using LCC, we have that (i) holds iff $c = xR_cL_cR_c^{-1} \cdot x^\rho = (c \cdot xE_c) \cdot x^\rho$, recalling $E_c = R_cL_cR_c^{-1}L_c^{-1}$ (see Lemma 2.11). Thus $(i) \leftrightarrow (iv)$. Interchanging c and x in this argument, we get $(ii) \leftrightarrow (v)$.

For $(iv) \leftrightarrow (vi)$, use Lemma 2.11(2) plus Lemma 2.9(3) to get:

$$(c \cdot xE_c)x^\rho = cx \cdot (x, c^\rho, c) \cdot x^\rho = cx \cdot x^\rho \cdot (x^\rho, c^\rho, c)^{-1} = c \cdot (c, x, x^\rho)(x^\rho, c^\rho, c)^{-1} \quad .$$

Interchanging c and x in this argument yields $(v) \leftrightarrow (vii)$. □

Corollary 3.3. *For a WIP element c of a CC-loop, $xE_c = x$ iff $cE_x = c$.*

Proof. By parts (iv) and (v) of Lemma 3.2. □

Theorem 3.4. *In a CC-loop Q, $W(Q)$ is a normal subloop.*

Proof. We show that $W = W(Q)$ is a subloop, so fix $b, c \in W$, and we show that W contains bc and c^ρ (see Lemma 2.12). Normality will follow from Lemma 2.1.

For bc: Set $u = c \cdot xc^\rho$, and note that $bu \cdot c = bc \cdot x$ by RCC, since $R_{c^\rho}L_cR_cL_c^{-1} = I$ (by Lemma 2.11(3): $E_c = R_cR_{c^\rho} = R_cL_cR_c^{-1}L_c^{-1}$). Then, using Lemma 3.2, $R_{c^\rho}L_c = L_cR_c^{-1}$, LCC, and $c \in W$, we have

$$b^\rho = u(bu)^\rho = ((cx)/c) \cdot (bu)^\rho = c \cdot x(c\backslash(bu)^\rho) = c \cdot x(bu \cdot c)^\rho = c \cdot x(bc \cdot x)^\rho.$$

Now

$$bc = (b^\rho)^\lambda c = (c \cdot x(bc \cdot x)^\rho)^\lambda c = (x(bc \cdot x)^\rho)^\lambda,$$

that is, $(bc)^\rho = x(bc \cdot x)^\rho$. By Lemma 3.2, $bc \in W$.

For c^ρ: By LCC,

$$c[(c\backslash x)x^\rho] = (x/c) \cdot cx^\rho = (cx^\rho)^\lambda \cdot cx^\rho = 1 \quad .$$

Then, using Lemma 2.11(3) ($E_{c^\rho} = L(c^\rho, c)^{-1} = L_c^{-1} L_{c^\rho}^{-1}$):

$$c^\rho = (c\backslash x)x^\rho = xE_{c^\rho}L_{c^\rho} \cdot x^\rho = (c^\rho \cdot xE_{c^\rho})x^\rho \quad ,$$

so c^ρ is WIP by Lemma 3.2. □

Corollary 3.5. *In a CC-loop Q, if $c \in W(Q)$, then $\langle c \rangle \subseteq W(Q)$.*

For a PACC-loop, we can say something about the structure of the quotient by the WIP subloop. To this end, we quote the following from [17], Theorem 8.4:

Theorem 3.6. *Let Q be a PACC-loop. For each $c \in Q$, $c^3 \in W(Q)$.*

Corollary 3.7. *Let Q be a PACC-loop with WIP subloop $W(Q)$. Then $Q/W(Q)$ is an elementary abelian 3-group.*

Then, since $N \le W$, we have:

Corollary 3.8. *If Q is a PACC-loop and $a^r \in N(Q)$, where $\gcd(r, 3) = 1$, then a is a WIP element.*

WIP elements have the following further associator properties:

Lemma 3.9. *In a CC-loop, if a is a WIP element and b is arbitrary, then $(a^2, x, y) = (b^2, u, v) = 1$ for all $x, y \in \langle a, b \rangle$ and all $u, v \in \langle a \rangle$. If b is also power-associative, then $(b^2, u, v) = 1$ for all $u, v \in \langle a, b \rangle$.*

Proof. By Lemma 3.2*(vi)* and *(vii)*, we have

$$(a, b, b^\rho) = (b^\rho, a, a^\rho) \qquad (a^\rho, b^\rho, b) = (b, a, a^\rho)$$

and

$$(b, a, a^\rho) = (a^\rho, b, b^\rho) \qquad (b^\rho, a, a^\rho) = (a^\rho, b, b^\rho)$$

so all these associators are equal. It follows by Lemma 2.9(4) that $(a^2, b, b^\rho) = 1$ and $(b^2, a, a^\rho) = 1$. By Lemma 2.9(5), we have $(a^2, x, y) = (b^2, u, v) = 1$ for all $x, y \in \langle b \rangle$ and all $u, v \in \langle a \rangle$.

Since b was arbitrary, we can also replace b by a to get $(a^2, x, y) = 1$ for all $x, y \in \langle a \rangle$. Then, by Lemma 2.9(1),

$$(a^2, a^\rho, b) = (a, a^\rho, b)T_a \cdot (a, a^\rho, b) = (a, b^\rho, b)T_a \cdot (a, b^\rho, b) = (a^2, b^\rho, b) = 1 \quad ,$$

so by Lemma 2.9(5), we have $(a^2, x, y) = 1$ for all $x \in \langle a \rangle$ and $y \in \langle b \rangle$. Applying Lemma 2.9(5) two more times, we get $(a^2, x, y) = 1$ for all $x, y \in \langle b \rangle$.

If b is also power-associative, then $(b^2, u, v) = 1$ for all $u, v \in \langle b \rangle$, and the above argument then gives us $(b^2, u, v) = 1$ for all $u, v \in \langle a, b \rangle$. □

This implies the following properties of 2-generated CC-loops when one of the generators has WIP. Parts of this lemma are in [17] (see Theorems 7.8, 7.10); the proof here is different.

Lemma 3.10. *Let Q be a CC-loop with nucleus $N = N(Q)$, and assume that $Q = \langle a, b\rangle N$ where a has WIP. Then $a^2 \in N$. Further,*

1. *If b is power-associative, then $b^2 \in N$ and $\langle a^2, b\rangle$ is a group.*
2. *If a and b are power-associative, then $\langle a, b^2\rangle$ is a group, $(a, a, b) = (a, b, b)$ generates $A(Q)$, $|A(Q)| \le 2$, Q is a PACC-loop, and $A(Q) \le Z(Q)$.*

Proof. First, $a^2 \in N$ by Lemma 3.9 because $(a^2, x, y) = 1$ for all $x, y \in Q$. Likewise, if b is power-associative then $b^2 \in N$ by Lemma 3.9, and $\langle a^2, b\rangle \le \langle \{b\} \cup N\rangle = \langle b\rangle N$ is a group.

Now assume that both a and b are power-associative. Then $\langle a, b^2\rangle$ is a group because $b^2 \in N$. By Theorem 1.1 and Lemmas 2.4 and 2.6, every associator in Q can be expressed in the form $(a^i b^j, a^k b^\ell, a^m b^n)$ for integers i, j, k, ℓ, m, n. Furthermore, since $a^2, b^2 \in N(Q)$, Lemma 2.6 implies the value of $(a^i b^j, a^k b^\ell, a^m b^n)$ depends only on i, j, k, ℓ, m, n mod 2.

Lemma 3.2 (vi) and (vii) now gives us $(a, a, b) = (a, b, b)$; call this value u. Then

$$u = (a, a, a)T_b \cdot (b, a, a) = (ab, a, a) = (a, a, a) \cdot (b, a, a)T_a = uT_a$$

by Lemma 2.9(1), so $(ab, a, a) = uT_a = u$; similarly, $(ab, b, b) = uT_b = u$. Then,

$$u^2 = (a, a, b) \cdot (a, a, b)T_a = (a^2, a, b) = 1 \quad .$$

Then $(ab, a, b) = (a, a, b)\cdot(b, a, b)T_a = u^2 = 1$ and $(ab, a, ab) = (a, a, ab)\cdot(b, a, ab)T_a = u$, and likewise $(ab, a, ab) = u$. Finally, $(ab, ab, ab) = (a, ab, ab) \cdot (b, ab, ab)T_a = u^2 = 1$. This accounts for all associators, so $A(Q) = \{1, u\}$.

Since $(x, x, x) = 1$ for each of $x = a, b, ab$, we have $(x, x, x) = 1$ for all x, so Q is a PACC-loop. Finally $u \in Z(Q)$ because u commutes with a and b. □

Corollary 3.11 ([17], Corollary 8.5)**.** *For each a, b in a PACC-loop, $\langle a^3, b^2\rangle$ and $\langle a^6, b\rangle$ are groups.*

Proof. By Theorem 3.6, a^3 has WIP, so the result follows from Lemma 3.10. □

4. Moufang, PseudoMoufang, and Extra Elements

Lemma 4.1. *Let Q be a CC-loop, and fix $a, b \in Q$. If any of the following hold, then they all hold:*

$$a \cdot ba = ab \cdot a \qquad (\text{Flex})$$

$$\begin{array}{llll} a \cdot ab = a^2 b & (\text{LAlt}) & ba \cdot a = ba^2 & (\text{RAlt}) \\ a^\lambda \cdot ab = b & (\text{LIP}) & ba \cdot a^\rho = b & (\text{RIP}) \\ \forall x\,[ab \cdot xa = a(bx \cdot a)] & (\text{Mfg1}) & \forall x\,[ax \cdot ba = (a \cdot xb)a] & (\text{Mfg2}) \\ \forall x\,[ab \cdot ax = a(ba \cdot x)] & (\text{F1}) & \forall x\,[xa \cdot ba = (x \cdot ab)a] & (\text{F2}) \end{array}$$

Proof. (Flex), (LAlt), and (RAlt) are equivalent by Lemma 2.8. (RIP) is $bE_a = b$, and Lemma 2.11(3) shows that this is equivalent to (LIP) and to (Flex). Taking $x = 1$ in (Mfg1) or in (F1) gives (Flex). To see that (Flex) $\to$ (F1 $\wedge$ Mfg1), apply LCC and (Flex) to get:

$$a(ba \cdot a\backslash u) = ((a \cdot ba)/a) \cdot (a \cdot a\backslash u) = ab \cdot u \quad .$$

Set $u = ax$ to get (F1). Setting $u = xa$ and applying RCC yields (Mfg1) by

$$ab \cdot xa = a(ba \cdot a\backslash xa) = a(bx \cdot a) \quad .$$

The equivalence with (Mfg2) and with (F2) is established similarly. □

If V is a variety of loops defined by some (universally quantified) equation, we may fix one variable of the equation and define an element c of an arbitrary loop to be a "V element" iff c satisfies that equation with the other variables quantified. For short, we simply say "c is V". We have already seen one example of this with WIP elements. For another, one of the Moufang equations is $\forall x, y, z\, [(z \cdot xy)z = zx \cdot yz]$, and Bruck defines c to be a Moufang element iff $\forall x, y\, [(c \cdot xy)c = cx \cdot yc]$ (see [4],VII§2). Of course, V may be defined by several equivalent equations, each of which may have several variables, so the proper definition of a "V element" is not uniquely determined. The following definitions seem to be useful in CC-loops.

Definition 4.2. *An element c of a CC-loop Q is a(n)*

$$\begin{array}{rcll} \text{Moufang element} & \textit{iff} & \begin{cases} \forall x, y\, [c(xy \cdot c) = cx \cdot yc] \\ \forall x, y\, [(c \cdot xy)c = cx \cdot yc] \end{cases} & (\text{Mfg}) \\ \text{pseudoMoufang element} & \textit{iff} & \begin{cases} \forall z, x\, [z(cx \cdot z) = zc \cdot xz] \\ \forall z, x\, [(z \cdot xc)z = zx \cdot cz] \end{cases} & (\text{PsM}) \\ \text{extra element} & \textit{iff} & \forall x, y\, [c(x \cdot yc) = (cx \cdot y)c] & (\text{Ex}) \end{array}$$

Let $M(Q)$, $P(Q)$, and $Ex(Q)$ denote the sets of Moufang, pseudoMoufang, and extra elements of Q, respectively.

In all loops, the two equations defining a Moufang element are equivalent because each one implies $\forall z\, [c \cdot zc = cz \cdot c]$. Note that (PsM) is obtained by fixing a different variable in the Moufang laws. In CC-loops, the two equations defining a Pseudo-Moufang element are equivalent because, by Lemma 4.1, (Mfg1) $\leftrightarrow$ (Mfg2).

Note that elements of $M(Q)$, $P(Q)$, and $Ex(Q)$ are power-associative.

The following is immediate from Lemmas 4.1 and 2.11(2).

Corollary 4.3. *Let c be an element of a CC-loop Q.*

(i) $c \in M(Q)$ *iff* $E_c = I$ *iff* $(x, c, c^\rho) = 1$ *for all* x.
(ii) $c \in P(Q)$ *iff* $cE_x = c$ *for all* x *iff* $(c, x, x^\rho) = 1$ *for all* x.

This corollary plus Lemma 2.9(5) yields the next two corollaries:

Corollary 4.4. *In a CC-loop Q, if $a \in M(Q) \cap P(Q)$ and b is a power-associative element, then $\langle a, b\rangle$ is a group.*

Corollary 4.5. *In a CC-loop Q, if $a \in M(Q)$ then $\langle a \rangle N(Q) \subseteq M(Q)$.*

Theorem 4.6. *In a CC-loop Q, $P(Q)$ is a normal subloop.*

Proof. $P(Q)$ is exactly the fixed point subset of the automorphisms E_x (Corollary 4.3*(ii)*), and thus is a subloop. Since $P(Q) \geq N(Q)$, the normality follows from Lemma 2.1. □

Lemma 4.7. *Let a, b be Moufang elements of a CC-loop Q. Then the following are equivalent:*

1. *ab is a Moufang element*	*2.* *ba is a Moufang element*
3. $(x, a, b) = (x, a^\rho, b)$ *for all* $x \in Q$	*4.* $(x, a, b) = (x, a, b^\rho)$ *for all* $x \in Q$

Proof. (1) $\leftrightarrow$ (2) holds by Corollary 4.5, because $[a, b] \in N(Q)$. For (1) $\leftrightarrow$ (3), note that $ab \in M(Q)$ iff $(x, ab, a^\rho b^\rho) = 1$ for all x (by Corollary 4.3), and

$$(x, ab, a^\rho b^\rho) = (x, a, a^\rho b^\rho)T_b \cdot (x, b, a^\rho b^\rho) =$$
$$(x, a, a^\rho)T_{b^\rho}T_b \cdot (x, a, b^\rho)T_b \cdot (x, b, b^\rho)T_{a^\rho} \cdot (x, b, a^\rho) = (x, a, b)^{-1} \cdot (x, b, a^\rho) \ ,$$

using $a, b \in M(Q)$ and Lemma 2.9. Similarly, (2) $\leftrightarrow$ (4). □

While we will use Lemma 4.7 below, we have not been able to show that $M(Q)$ is a subloop even in the power-associative case. Thus we offer the following.

Conjecture 4.8. *There exists a PACC-loop Q in which $M(Q)$ is not a subloop.*

Note that by Lemma 4.14 below, such a Q cannot be WIP.

Extra loops, introduced by Fenyves [12, 13], are loops satisfying one of the following three equivalent identities:

$$zx \cdot zy = z(xz \cdot y) \qquad xz \cdot yz = (x \cdot zy)z \qquad z(x \cdot yz) = (zx \cdot y)z \ .$$

The identities (F1) and (F2) in Lemma 4.1 are obtained by fixing variables in the first two of these, but for our definition of "extra element", we found it more useful to fix a variable in the third one. Extra loops are both CC and Moufang, and all squares in an extra loop are nuclear. Generalizing this,

Lemma 4.9. *For an element c of a CC-loop Q, the following are equivalent:*

(i) *c is extra*

(ii) $\forall x, y\, [c(x \cdot cy) = (cx \cdot c)y]$	*(iii)* $\forall x, y\, [(yc \cdot x)c = y(c \cdot xc)]$
(iv) $\forall x, y\, [c(x \cdot cy) = (c \cdot xc)y]$	*(v)* $\forall x, y\, [(yc \cdot x)c = y(cx \cdot c)]$

(vi) *c is Moufang and* $c^2 \in N(Q)$

Proof. First note that (i)–(v) imply that $c \cdot xc = cx \cdot c$ (setting $y = 1$ in (Ex) or (ii)–(v)). Thus, by Lemma 4.1, in all cases, c is Moufang, and hence also $c \cdot cx = c^2 x$ (i.e., $L_c^2 = L_{c^2}$). (ii)$\leftrightarrow$(iv) and (iii)$\leftrightarrow$(v) follow from $c \cdot xc = cx \cdot c$.

For (i)$\leftrightarrow$(vi), note that c is extra iff $A(c) := (L_c, R_c^{-1}, L_c R_c^{-1})$ is an autotopism, and c is Moufang iff $B(c) := (L_c, R_c, R_c L_c)$ is an autotopism. Since c *is* Moufang, $D(c) := A(c)B(c) = (L_{c^2}, I, L_{c^2})$, and c is extra iff $D(c)$ is an autotopism iff $c^2 \in N$.

Now, (ii) holds iff $H(c) := (L_cR_c, L_c^{-1}, L_c)$ is an autotopism, and c Moufang implies that $F(c) := (R_c, L_c^{-1}R_c, R_c)$ is an autotopism (see (F2) in Lemma 4.1). Then (i)$\leftrightarrow$(ii) follows from $H(c) = A(c)F(c)$ (using $L_cR_c = R_cL_c$). (i)$\leftrightarrow$(iii) is similar. □

Lemma 4.10. *In a CC-loop Q, let a be an extra element and let b be a Moufang element. Then ab and ba are Moufang elements.*

Proof. By Lemma 4.9, a is Moufang and $a^2 \in N(Q)$. By Lemma 2.6(1), $(x, a^\rho, b) = (x, a^2a^\rho, b) = (x, a, b)$. Now use Lemma 4.7. □

Lemma 4.11. *In a CC-loop Q, $S(Q) := \{a : a^2 \in N(Q)\}$ is a normal subloop.*

Proof. If $a, b \in Q$, then by Theorem 1.1, there exists $n_1, n_2 \in N$ such that $(ab)^2 = (a^2b^2)n_1$ and $(a^\rho)^2 = (a^2)^\rho n_2$. Thus $a, b \in S$ implies $ab, a^\rho \in S$, and so S is a subloop by Lemma 2.12. Normality follows from Lemma 2.1. □

Theorem 4.12. *In a CC-loop Q, $Ex(Q)$ is a normal subloop.*

Proof. Fix $a, b \in Ex(Q)$. By Lemmas 4.9 and 4.10, ab is Moufang. By Lemmas 4.9 and 4.11, $(ab)^2 \in N$, so $ab \in Ex(Q)$. Next $a^{-1} \in Ex(Q)$ by Corollary 4.5. Thus $Ex(Q)$ is a normal subloop by Lemmas 2.1 and 2.12. □

Now we relate Moufang and pseudoMoufang elements to WIP elements, after first proving a technical lemma.

Lemma 4.13. *Let c be an element of a CC-loop. The following are equivalent: (i) c is pseudoMoufang, (ii) $cx = (cx \cdot yx^\rho) \cdot xy^\rho$ for all x, y, (iii) $xc = y^\lambda x \cdot (x^\lambda y \cdot xc)$ for all x, y.*

Proof. $(ii) \to (i)$ follows from taking $x = 1$ and using Corollary 4.3(ii).

For $(i) \to (ii)$: We start with the equation $x = (x \cdot yx^\rho) \cdot xy^\rho$ ([17], Lemma 5.1). Define u, v by the equations $yx^\rho = (u)T_x$ and $xy^\rho = (v)T_x$. Then $x = ux \cdot (v)T_x = uv \cdot x$ using RCC. Thus $uv = 1$, and so by Corollary 4.3(ii), $c = cE_u = cu \cdot v$. Hence $cx = (cu \cdot v)x = (cu \cdot x) \cdot xy^\rho = (cx \cdot yx^\rho) \cdot xy^\rho$ using RCC twice.

The proof of $(i) \leftrightarrow (iii)$ is just the mirror of the preceding argument. □

Lemma 4.14. *Let c be an element of a CC-loop. Any two of the following properties imply the third: (i) c is a WIP element, (ii) c is Moufang, (iii) c is pseudoMoufang. In case these conditions hold, c is extra.*

Proof. If c is a WIP element, then (ii) and (iii) are equivalent by Corollaries 3.3 and 4.3. If c is Moufang and pseudoMoufang, then $c = cE_x = (c \cdot xE_c) \cdot x^\rho$, and so c is WIP by Lemma 3.2.

Now suppose c satisfies (i), (ii), and (iii). Since c^{-1} is pseudoMoufang (Theorem 4.6), we have $c^{-1}x = (c^{-1}x \cdot yx^\rho) \cdot xy^\rho$ for all x, y, by Lemma 4.13. Replacing x with cx and using $c^{-1} \cdot cx = x$ (Corollary 4.3(i)), we obtain $x = [x \cdot y(cx)^\rho](cx \cdot y^\rho)$. Now $(cx)^\rho = x\backslash c^{-1}$ by Lemma 3.2, and so $x = [x \cdot y(x\backslash c^{-1})](cx \cdot y^\rho) = ((xy)/x)c^{-1} \cdot (cx \cdot y^\rho)$, using LCC. Thus $xc = [((xy)/x)c^{-1} \cdot c](c\backslash[(cx \cdot y^\rho)c]) = ((xy)/x)(c\backslash[(cx \cdot y^\rho)c])$ by RCC and Corollary 4.3(1) again. Using LCC again, $xc = x \cdot y\{x\backslash(c\backslash[(cx \cdot y^\rho)c])\}$. Cancelling x's and rearranging, we have $(cx \cdot y^\rho)c = c(x(y\backslash c)) = c(x \cdot y^\rho c)$ by Corollary 4.3(2). Replacing y with y^λ establishes the desired result. □

Example 4.15. The converse of Lemma 4.14 is not true, since in a CC-loop, extra elements need not be WIP. For the CC-loop Q in Table 1, $Z(Q) = \{0, 1\}$, $N(Q) = W(Q) = \{0, 1, 2, 3\}$, $Ex(Q) = M(Q) = \{0, 1, 2, 3, 4, 5, 6, 7\}$, and $P(Q) = \{0, 1, 2, 3, 8, 9, 10, 11\}$. For example, 4 is extra but not WIP because $4 \cdot (8 \cdot 4)^\rho = 4 \cdot 14^\rho = 4 \cdot 13 = 9 \neq 8^\rho = 8$. The set of power-associative elements of this loop is $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$, which is not a subloop. We also see that Theorem 3.6 cannot be improved; that is, in a PACC-loop, $W(Q)$ contains all cubes, but in this loop, 4 is power-associative, and $4^3 = 4 \notin W(Q)$. This example was produced by the program Mace4 [19]; as usual, given the example, it is trivial to verify its properties using a standard programming language.

Q	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	0	3	2	5	4	7	6	9	8	11	10	13	12	15	14
2	2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13
3	3	2	1	0	7	6	5	4	11	10	9	8	15	14	13	12
4	4	5	6	7	0	1	2	3	12	13	14	15	8	9	10	11
5	5	4	7	6	1	0	3	2	13	12	15	14	9	8	11	10
6	6	7	4	5	2	3	0	1	14	15	12	13	10	11	8	9
7	7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8
8	8	9	11	10	14	15	13	12	0	1	3	2	6	7	5	4
9	9	8	10	11	15	14	12	13	1	0	2	3	7	6	4	5
10	10	11	9	8	12	13	15	14	2	3	1	0	4	5	7	6
11	11	10	8	9	13	12	14	15	3	2	0	1	5	4	6	7
12	12	13	15	14	10	11	9	8	5	4	6	7	3	2	0	1
13	13	12	14	15	11	10	8	9	4	5	7	6	2	3	1	0
14	14	15	13	12	8	9	11	10	7	6	4	5	1	0	2	3
15	15	14	12	13	9	8	10	11	6	7	5	4	0	1	3	2

TABLE 1. extra $\not\to$ WIP

In the power-associative case, however, the converse of Lemma 4.14 does hold, and the pseudoMoufang elements coincide with the extra elements.

Lemma 4.16. *If Q is a PACC-loop, then $P(Q) = Ex(Q) \leq W(Q)$.*

Proof. For $Ex(Q) \leq W(Q)$: if $c \in Q$ is extra, then $c^2 \in N(Q)$ (Lemma 4.9) and $c^3 \in W(Q)$ (Theorem 3.6), and so $c = c^3 \cdot c^{-2} \in W(Q)$ by Theorem 3.4.

For $P(Q) \le W(Q)$: if $c \in Q$ is pseudoMoufang, then $cx \cdot x^{-1} = c = cx \cdot (cx)^{-1}c$ for all x by Corollary 4.3. Cancel the cx to get that c is WIP.

Finally, $Ex(Q) = P(Q)$ follows from Lemmas 4.14 and 4.9. □

Corollary 4.17. *Let a, b be elements of a PACC-loop, and suppose a is extra. Then $\langle a, b\rangle$ is a group.*

Proof. By Lemmas 4.9, 4.16, and 4.14, a is both Moufang and pseudoMoufang. Now apply Corollary 4.4. □

We insert here some criteria for determining when a PACC-loop is WIP.

Lemma 4.18. *Let Q be a PACC-loop. The following are equivalent: (i) Q is WIP, (ii) every square is nuclear, (iii) every square is extra, (iv) every square is Moufang, (v) every square is pseudoMoufang, (vi) every square is WIP.*

Proof. (i)→(ii) is due essentially to Басараб [1], and is true in any CC-loop; see also [17], §7. (ii)→(iii) is clear from the definitions, and (iii)→(iv) follows from Lemma 4.9.

(iv)→(v): By (iv) and Lemma 2.11(4), $E_y^4 = E_{y^2} = I$. Since $\langle x^2, y^3\rangle$ is a group (by Corollary 3.11), $x^2E_y = x^2E_y^9 = x^2E_{y^3} = x^2$, so x^2 is pseudoMoufang.

(v)→(vi) is from Lemma 4.16.

(vi)→(i): Each $x^3 \in W(Q)$ by Theorem 3.6. Thus each $x = x^3 \cdot x^{-2} \in W(Q)$ by Theorem 3.4. □

We now turn to the main results of this section.

Theorem 4.19. *In a CC-loop Q, if $c \in W(Q)$, then $c^2 \in Ex(Q)$ and $c^2c^2 \in N(Q)$.*

Proof. For each $x \in Q$, $c^2 \in N(\langle c, x\rangle)$ by Lemma 3.10. Thus c^2 is Moufang, and so by Lemma 4.14, c^2 is extra. The rest follows from Lemma 4.9. □

Incidentally, by Lemma 3.10, $c \cdot cc^2 = c^2c^2 = c^2c \cdot c$; however, $c \cdot c^2$ need not equal $c^2 \cdot c$. Thus, the final part of the conclusion of Theorem 4.19 would have been ambiguous if written as $c^4 \in N(Q)$.

Theorem 4.20. *For all c in a PACC-loop Q,*

1. c^3 *is a WIP element*
2. c^6 *is an extra element*
3. $c^{12} \in N(Q)$

In particular, if c has finite order prime to 6, then $c \in N(Q)$.

Proof. (1) just restates Theorem 3.6, and apply Theorem 4.19 for the rest. □

Note that Theorem 4.20(2) and Corollary 4.17 give a different proof of part of Corollary 3.11. We now have:

Corollary 4.21. *Let Q be a PACC-loop.*

1. $Q/W(Q)$ *is an elementary abelian* 3*-group.*

2. *$Q/Ex(Q)$ is an abelian group of exponent* 6.
3. *$Q/N(Q)$ is an abelian group of exponent* 12.

5. Fat Nuclei

Following up on Corollary 4.21(3), in this section we consider the minimal possibilities for $Q/N(Q)$ for PACC-loops Q.

Lemma 5.1. *If Q is a PACC-loop, $G \le Q$ is a group, and $GN = Q$, then Q is a group.*

Proof. The set $G \cup N$ associates, so $\langle G \cup N\rangle$ is a group; see ([17], Corollary 6.4). □

Corollary 5.2. *A PACC-loop Q with Q/N cyclic is a group.*

The following two lemmas are especially useful for PACC-loops in which the center coincides with the nucleus.

Lemma 5.3. *Let $Q = \langle a, b\rangle$ be a PACC-loop, and assume $bE_a = bu$ and $aE_b = av$ where $u, v \in Z(Q)$. Then $u^3 = v^3$, $u^6 = v^6 = 1$, and*

$$(a^i b^j, a^k b^\ell, a^m b^n) = u^{-ikn-i\ell m-jkm} v^{-i\ell n-jkn-j\ell m} \tag{†}$$

for all integers i, j, k, ℓ, m, n. Also, $a^6, b^6 \in N(Q)$ and $A(Q) = \langle u, v\rangle \le Z(Q)$.

Proof. Since $E_a^6 = E_b^6 = I$ (Lemma 2.11(5)), we have $u^6 = v^6 = 1$. Now $u = (b, a, a^{-1}) = (a, a, b)^{-1}$ and $v = (a, b, b^{-1}) = (a, b, b)^{-1}$ by Lemmas 2.11(2) and 2.9(3). Applying Lemma 2.9(1)(3) and multiple inductions, we get

$$\begin{aligned}(a^i b^j, a^k b^\ell, a^m b^n) &= (a, a, b)^{ikn+i\ell m+jkm}(a, b, b)^{i\ell n+jkn+j\ell m}\\ &= u^{-ikn-i\ell m-jkm} v^{-i\ell n-jkn-j\ell m}.\end{aligned}$$

Now if $i = j = k = \ell = m = n = 1$, we have $1 = (ab, ab, ab) = u^{-3}v^{-3}$, and when combined with $u^6 = v^6 = 1$, this gives $u^3 = v^3$. By Theorem 1.1 and Lemmas 2.4 and 2.6, every associator in Q can be expressed in the form (†), and so $A(Q) = \langle u, v\rangle \le Z(Q)$. Taking $i = 6$, $j = 0$ in (†) gives $a^6 \in N(Q)$, and similarly, $b^6 \in N(Q)$. □

Corollary 5.4. *Let Q be a 2-generated PACC-loop with $A(Q) \le Z(Q)$. Then $Q/N(Q)$ is an abelian group of exponent* 6.

Lemma 5.5. *Let $Q = \langle a, b\rangle$ be a PACC-loop satisfying the hypotheses of Lemma 5.3. In addition, assume $ba = abz$ where $z = [b, a] \in Z(Q)$. Then*

$$b^i a^j = a^j b^i \cdot z^{ij} u^{i(j-1)j/2} v^{-j(i-1)i/2}\ , \tag{Z1}$$

and

$$a^i b^j \cdot a^k b^\ell = a^{i+k} b^{j+\ell} \cdot z^{jk} u^{i\ell k + j(k-1)k/2} v^{-ij\ell - k(j-1)j/2} \tag{Z2}$$

for all integers i, j, k, ℓ.

Proof. We first prove the following special cases of (Z1):

$$ba^j = a^j b \cdot z^j u^{(j-1)j/2} \qquad \text{(Z3)} \qquad\qquad b^i a = ab^i \cdot z^i v^{-(i-1)i/2} \qquad \text{(Z4)}$$

Now (Z3) is clear for $j = 1$, and proceeding by induction, using Lemma 5.3:

$$\begin{aligned} ba^{j+1} &= ba \cdot a^j \cdot (b, a, a^j)^{-1} = abz \cdot a^j \cdot u^j = a \cdot ba^j \cdot (a, b, a^j) \cdot zu^j \\ &= a \cdot a^j b \cdot z^j u^{(j-1)j/2} \cdot (a, a^j, b) \cdot zu^j = a^{j+1} b \cdot z^{j+1} u^{j(j+1)/2} \end{aligned}$$

The mirror of this argument yields (Z4). Now, in (Z3), we can replace b by b^i, replace z by $z^i v^{-(i-1)i/2}$ (using (Z4)), and replace u by u^i (since $(b^i)E_a = b^i u^i$) to get (Z1).

For (Z2), we repeatedly use Lemma 5.3, (Z1) and (Z2) to compute

$$\begin{aligned} a^i b^j \cdot a^k b^\ell &= a^i \cdot (b^j \cdot a^k b^\ell) \cdot (a^i, b^j, a^k b^\ell) \\ &= a^i (b^j a^k \cdot b^\ell) \cdot (b^j, a^k, b^\ell)^{-1} \cdot u^{-ijk} v^{-ij\ell} \\ &= a^i (a^k b^j \cdot b^\ell) \cdot z^{jk} u^{j(k-1)k/2} v^{-k(j-1)j/2} \cdot (b^j, a^k, b^\ell)^{-1} \cdot u^{-ijk} v^{-ij\ell} \\ &= a^i \cdot a^k b^{j+\ell} \cdot z^{jk} u^{-ijk+j(k-1)k/2} v^{-ij\ell-k(j-1)j/2} \\ &= a^{i+k} b^{j+\ell} \cdot (a^i, a^k, b^{j+\ell})^{-1} \cdot z^{jk} u^{-ijk+j(k-1)k/2} v^{-ij\ell-k(j-1)j/2} \\ &= a^{i+k} b^{j+\ell} \cdot z^{jk} u^{i\ell k+j(k-1)k/2} v^{-ij\ell-k(j-1)j/2} \end{aligned}$$

□

In Theorem 7.9, we will construct loops satisfying the hypotheses of Lemma 5.5.

Lemma 5.6. *Let $Q = \langle a, b\rangle$ be a PACC-loop satisfying the hypotheses of Lemma 5.5, and assume also that $a^3 \in Z(Q)$. Then $u^3 = v^3 = z^3 = 1$ and $b^3 \in Z(Q)$.*

Proof. By Lemma 5.5(Z1), if $a^3 \in Z(Q)$, then $1 = z^{3i} u^{3i} v^{-3(i-1)i/2}$ for all i. Taking $i = 1$, we have $1 = z^3 u^3$. Since $u^6 = 1$, $z^3 = u^3$. Then taking $i = 2$, we get $1 = z^6 u^6 v^{-3} = v^{-3}$, and so $v^3 = 1$, and so $u^3 = z^3 = 1$ by Lemma 5.3. That $b^3 \in Z(Q)$ then follows from Lemma 5.5(Z2). □

Lemma 5.7. *Let $Q = \langle a, b\rangle$ be a PACC-loop satisfying the hypotheses of Lemma 5.5, and assume also that $a^2, b^2 \in Z(Q)$. Then $u = v = z^2$ and $u^2 = z^4 = 1$.*

Proof. By Lemma 5.5(Z1), if $a^2 \in Z(Q)$, then $1 = z^{2i} u^i v^{-(i-1)i}$ for all i. Taking $i = 1$, we have $1 = z^2 u$, and so $u = z^{-2}$. Taking $i = 2$, we get $1 = z^4 u^2 v^{-2} = v^{-2}$. Next, $b^2 \in Z(Q)$ gives $1 = z^{2j} u^{(j-1)j} v^{-j}$ for all j. Taking $j = 1$ gives $1 = z^2 v^{-1} = z^2 v$, and so $u = z^{-2} = v$ and $u^2 = z^{-4} = v^2 = 1$. □

Since $[a, b] \in N(Q)$ always holds in a CC-loop (Theorem 1.1), we have:

Corollary 5.8. *Let Q be a PACC-loop.*

1. *If $Z(Q)$ is an elementary abelian 2-group and $A(Q) \leq Z$, then Q is WIP.*
2. *If $N = Z$ is an elementary abelian 2-group, then Q is extra.*

Proof. For (1): fix $a, b \in Q$ and adopt the notation of Lemma 5.3. Then $u = v$ and $u^2 = v^2 = 1$. By Lemma 2.11(4), $bE_{a^2} = bE_a^4 = b$, and so every square is Moufang. By Lemma 4.18, Q is WIP.

For (2): $N = Z$ being an elementary abelian 2-group, and Theorem 1.1 imply the hypotheses of (1), so that Q is WIP. Thus squares are central by Lemma 4.18. Fixing $a, b \in Q$, Lemma 5.7 implies $u = v = z^2 = 1$. Hence $\{a, b\}$ associates so that $\langle a, b\rangle$ is a group, *i.e.*, Q is extra. □

Corollary 5.9. *If Q is a PACC-loop of order 8, then Q is a group.*

Proof. Otherwise, by Corollaries 5.2 and 5.8, $|N| = 2$ and Q is an extra loop, but the smallest nonassociative extra loop has order 16 (see [16, 17], or [5]). □

We conclude this section by examining the case $|Q/N| = 4$ in some detail.

Lemma 5.10. *Assume that Q is a PACC-loop with $|Q/N| = 4$. Then Q/N is an elementary abelian 2-group, and Q has WIP. If $Q/N = \{N, Na, Nb, Nab\}$, then $A(Q) = \{1, u\} \leq Z(Q)$, where $u = (a, a, b) = (a, b, b) \neq 1$. Also, 4 divides $|N|$.*

Proof. Q/N is an elementary abelian 2-group by Corollary 4.21(1) (or by Lemma 3.10), and Q has WIP by Corollary 3.8. The claim about $A(Q)$ follows from Lemma 3.10.

Now suppose that $|N| = 2r$, where r is odd, so $|Q| = 8r$. Let $G = Q/A$, and let $\pi : Q \twoheadrightarrow G$ be the quotient map. G is a group of order $4r$ and $\pi(N) \trianglelefteq G$, with $|\pi(N)| = r$. Let P be a Sylow 2-subgroup of G. Then $|P| = 4$, and P contains exactly one element from each of the four cosets of $\pi(N)$. Say $P = \{1, \pi(n_1a), \pi(n_2b), \pi(n_3ab)\}$, with $n_1, n_2, n_3 \in N$. Then $\pi^{-1}(P)$ is a subloop of Q of order 8. Since $(n_1a, n_1a, n_2b) = (a, a, b) = u \neq 1$, $\pi^{-1}(P)$ is nonassociative, contradicting Corollary 5.9. □

6. Orders

There are nonassociative PACC-loops of order 16 (the five extra loops plus three others; see §8) and of order 27 (see §9). By taking products with a group of order n, we get nonassociative PACC-loops of order $16n$ and $27n$ for all finite $n \geq 1$. These are the only possible finite orders by Theorem 6.4 below.

Lemma 6.1. *Let Q be a PACC-loop with finite associator subloop $A = A(Q)$. Let n be an integer relatively prime to $|A|$.*

1. *If $a \in Q$ satisfies $E_a^n = I$, then $E_a = I$.*
2. *If $a \in Q$ satisfies $E_{a^n} = I$, then $E_a = I$.*

Proof. For (1): For each $x \in Q$, $(x)E_a = xu$ where $u = (x, a, a^{-1})$. Thus $x = (x)E_a^n = xu^n$, and $u^n = 1$. Since n is prime to $|A|$, $u = 1$.

For (2): this follows from (1) and $E_{a^n} = E_a^{n^2}$. □

Lemma 6.2. *Let Q be a finite PACC-loop, and suppose $|A(Q)|$ is relatively prime to $|Q/N(Q)|$. Then Q is a group.*

Proof. For each $a \in Q$, we have $a^k \in N$ for some k relatively prime to $|A|$. Thus $E_{a^k} = I$, and so $E_a = I$ by Lemma 6.1. Therefore Q is Moufang (Corollary 4.3(i)), and hence an extra loop. But in an extra loop, A and Q/N are elementary abelian 2-groups [16], and so Q must be a group. $\square$

Lemma 6.3. *If Q is a finite PACC-loop and $3 \nmid |A(Q)|$, then Q is WIP.*

Proof. First, fix any $x, y \in Q$. Then $yE_x = yn$ for some $n \in A$. $E_x^6 = I$ implies $n^6 = 1$, but then $n^2 = 1$ since $3 \nmid |A|$. Thus, $E_x^2 = I$ for all x, and hence also $E_{x^2} = E_x^4 = I$. Thus, Q is WIP by Lemma 4.18 and Corollary 4.3. $\square$

Theorem 6.4. *Let Q be a finite, nonassociative PACC-loop. If Q is WIP, then $16 \mid |Q|$. If Q is not WIP, then $27 \mid |Q|$.*

Proof. If Q is WIP, then $x^4 \in N$ for all x by Theorem 4.19. Thus, $|Q/N| = 2^k$ for some $k \geq 2$ by Corollary 5.2, and $2 \mid |N|$ by Lemma 6.2, so $16 \mid |Q|$ unless $4 \nmid |N|$ and $|Q/N| = 4$; but this would contradict Lemma 5.10.

If Q is not WIP, fix $b \notin W$. Say $o(b) = 3^j k$, where $\gcd(3, k) = 1$. Then $b^k \notin W$ by Corollary 3.7, and so replacing b by b^k if necessary, WLOG assume that $o(b) = 3^j$. Now fix a such that $b(ab)^{-1} \neq a^{-1}$. Then $a \notin \langle b \rangle W$. To see this, suppose that $a = b^i w$ for $w \in W$ and $i \in \mathbb{Z}$. Then $a, b \in \langle w, b^2 \rangle$ (since $o(b) = 3^j$), and $\langle w, b^2 \rangle$ is a group by Lemma 3.10, contradicting $b(ab)^{-1} \neq a^{-1}$.

Thus, $9 \mid |Q/W|$. Since $3 \mid |A|$ by Lemma 6.3, $3 \mid |W|$, and so $27 \mid |Q|$. $\square$

7. Extension

Here, we show how in some cases, the equations of Lemma 5.3 may be used as a prescription for constructing a PACC-loop. This will be useful in Sections 8 and 9, where we construct all PACC-loops of a given order. The natural converse to Lemma 5.5 would be:

Lemma 7.1. *Assume that Q is a PACC-loop, $a, b \in Q$, and $z, u, v \in Z(Q)$, with*

$$a^i b^j \cdot a^k b^\ell = a^{i+k} b^{j+\ell} \cdot z^{jk} u^{j(k-1)k/2} v^{-k(j-1)j/2} \cdot u^{i\ell k} v^{-ij\ell}$$

holding for all $i, j, k, \ell \in \mathbb{Z}$. Then $ba = abz$, $(b)E_a = bu$, and $(a)E_b = av$.

Proof. Setting $j = k = 1$ and $i = \ell = 0$, we get $ba = abz$. Also,

$$(b)E_a = ba \cdot a^{-1} = ab \cdot a^{-1} \cdot z = b \cdot z^{-1} u \cdot z = bu$$

(setting $i = j = 1, k = -1, \ell = 0$), and

$$(a)E_b = ab \cdot b^{-1} = a \cdot v$$

(setting $i = j = 1, k = 0, \ell = -1$). $\square$

We now consider how to build such loops. First, a more general construction; the following is a variant of the construction described in [16] (see Definition 7.1 and Lemmas 7.2 and 7.3):

Definition 7.2. *Say we are given abelian groups $(A,+)$ and $(G,+)$, and a function $f : A \times A \to G$, satisfying*

$$f(0,a) = f(a,0) = 0 \quad \textit{for all } a \in A \quad . \tag{$*1$}$$

Then $A \ltimes_f G$ is the set $Q = A \times G$ with a product defined by:

$$(a,x) \cdot (b,y) = (a+b,\ x+y+f(a,b)) \quad .$$

Lemma 7.3. *Let $Q = A \ltimes_f G$, where f satisfies $(*1)$. Then Q is a loop with identity element $(0,0)$ and divisions given by:*

$$\begin{aligned} (c,z)/(b,y) &= (c-b,\ z-y-f(c-b,b)) \\ (a,x)\backslash(c,z) &= (c-a,\ z-x-f(a,c-a)) \quad . \end{aligned}$$

Associators are given by

$$((a,x),(b,y),(c,z)) = \big(0,\ \mathcal{A}_f(a,b,c)\big) \quad ,$$

where

$$\mathcal{A}_f(a,b,c) := f(a,b) + f(a+b,c) - f(b,c) - f(a,b+c).$$

Commutators are given by

$$[(b,y),(a,x)] = (0, f(b,a) - f(a,b)) \quad ,$$

and so

$$(b,y)T_{(a,x)} = (b,y) \cdot (0, f(b,a) - f(a,b)) \quad .$$

Also, $G \cong \{0\} \times G \leq Z(Q)$.

Proof. The division formulas are obtained by solving $(a,x)\cdot(b,y) = (c,z)$ for (a,x) and for (b,y). It is clear that elements of $\{0\} \times G$ commute with all elements of Q. To show that $\{0\} \times G \leq N(Q)$ (and hence $\{0\} \times G \leq Z(Q)$), note

$$\begin{aligned} (a,x)\cdot(b,y)(c,z) &= (a+b+c,\ x+y+z+f(b,c)+f(a,b+c)) \\ (a,x)(b,y)\cdot(c,z) &= (a+b+c,\ x+y+z+f(a,b)+f(a+b,c)) \quad . \end{aligned}$$

These two are equal if at least one of a,b,c is 0. Thus, $\{0\} \times G \leq N(Q)$. Dividing the expressions for products, we get the formula for associators. Finally,

$$(b,y)\cdot(a,x) = (a,x)\cdot(b,y)\cdot(0, f(b,a) - f(a,b)) \quad .$$

yields the formulas for commutators and for the mappings $T_{(a,x)} = R_{(a,x)} L_{(a,x)}^{-1}$. □

Definition 7.4. *If A, G be abelian groups, then a mapping $f : A \times A \to G$ is*

- CC-good *if f satisfies $(*1)$ and $A \ltimes_f G$ is a CC-loop.*
- PACC-good *if f satisfies $(*1)$ and $A \ltimes_f G$ is a PACC-loop.*

The characterization of associators in Lemma 7.3 gives us:

Lemma 7.5. *Let A, G be abelian groups, and assume $f : A \times A \to G$ satisfies $(*1)$. Then f is CC-good iff $\mathcal{A}_f(a,b,c)$ is invariant under permutations of $\{a,b,c\}$. In that case, $(a,x) \in Z(A \ltimes_f G)$ iff $f(a,b) = f(b,a)$ for all b.*

Proof. Since $A \ltimes_f G$ clearly satisfies (b) of Lemma 2.8, CC is equivalent to (a), which is equivalent to the invariance of $\mathcal{A}_f(a,b,c)$ under permutations. Then, note that for CC-loops, $(a,x) \in Z(Q)$ iff (a,x) commutes with all other elements, and apply the characterization of commutators in Lemma 7.3. $\square$

Lemma 7.6. *Let A, G be abelian groups, and assume $f : A \times A \to G$ is CC-good. Then f is PACC-good iff $\mathcal{A}_f(a,a,a) = 0$ for all $a \in A$. In that case, $f(ma, na) = f(na, ma)$ for all $a \in A$ and all $m, n \in \mathbb{Z}$.*

Proof. By Lemma 1.3, (x,a) is a power-associative element of $A \ltimes_f G$ iff $(0,0) = ((x,a),(x,a),(x,a)) = (0, \mathcal{A}_f(a,a,a))$. The rest follows since $(a,x)^m$ and $(a,x)^n$ must commute in a power-associative loop. $\square$

Lemma 7.7. *If A, G are abelian groups, then the sets of all CC-good and PACC-good $f : A \times A \to G$ are subgroups of $G^{A\times A}$.*

Proof. If $f, g : A \times A \to G$ satisfy $(*1)$, then obviously so does $f + g$. The rest follows from Lemmas 7.5, 7.6, and the observation that $\mathcal{A}_{f+g}(a,b,c) = \mathcal{A}_f(a,b,c) + \mathcal{A}_g(a,b,c)$ for all $a,b,c \in A$. $\square$

Lemma 7.8. *If A, G are abelian groups and $f : A \times A \to G$ is bilinear, then f is PACC-good and $A \ltimes_f G$ is a group.*

Motivated now by Lemma 7.1, we start with $A = \langle a \rangle \times \langle b \rangle \cong \mathbb{Z} \times \mathbb{Z}$, and let G be some abelian group containing elements z, u, v. Converting to additive notation, we define $f : A \times A \to G$ by:

$$f(ia + jb, ka + \ell b) = (j(k-1)k/2 + i\ell k)u + (-k(j-1)j/2 - ij\ell)v + (jk)z \quad . \quad (*2)$$

This is a well-defined function since a and b are assumed to have infinite order. Then, if it is desired to construct a finite loop, we will quotient out a suitable normal subloop of $A \ltimes_f G$.

Theorem 7.9. *Let G be an abelian group and $A = \langle a \rangle \times \langle b \rangle \cong \mathbb{Z} \times \mathbb{Z}$. Fix $z, u, v \in G$ and define f as in $(*2)$, and let $P = A \ltimes_f G$. Then P is a CC-loop. In addition, P is a PACC-loop iff $3u = 3v$ and $6u = 6v = 0$. In this case, $6a, 6b \in N(P)$.*

Proof. First, observe that the mapping $f_z(ia + jb, ka + \ell b) = (jk)z$ is bilinear, and hence PACC-good by Lemma 7.8.

Next, consider $f_u(ia + jb, ka + \ell b) = (j(k-1)k/2 + i\ell k)u$. We compute $\mathcal{A}_{f_u}$:

$$\begin{aligned}
&\mathcal{A}_{f_u}(ia + jb, ka + \ell b, pa + qb) = \\
&f_u(ia + jb, ka + \ell b) + f_u((i+k)a + (j+\ell)b, pa + qb) - \\
&f_u(ka + \ell b, pa + qb) - f_u(ia + jb, (k+p)a + (\ell+q)b) = \\
&(j(k-1)k/2 + ik\ell)u + ((j+\ell)p(p-1)/2 + (i+k)pq)u - \\
&(\ell p(p-1)/2 + kpq)u - (j(k+p-1)(k+p)/2 + i(k+p)(\ell+q))u = \\
&(-ikq - jkp - i\ell p)u \quad .
\end{aligned}$$

Thus $\mathcal{A}_{f_u}$ is invariant under permutation of its arguments, and so f_u is CC-good by Lemma 7.5.

Similarly, for $f_v(ia+jb, ka+\ell b) = (-k(j-1)j/2 - ij\ell)v$, we find that $\mathcal{A}_{f_v}(ia+jb, ka+\ell b, pa+qb) = -i\ell p - j\ell q - jkq$, and so f_v is CC-good by Lemma 7.5.

Since $f = f_u + f_v + f_z$, f is CC-good by Lemma 7.7.

Now $\mathcal{A}_f = \mathcal{A}_{f_u} + \mathcal{A}_{f_v}$, and so $\mathcal{A}_f(ia+jb, ia+jb, ia+jb) = -3i^2ju - 3ij^2v = -3ij(iu+jv)$ for all i, j. If f is PACC-good, then $-3ij(iu+jv) = 0$ for all i, j by Lemma 7.6. Taking $i = -j = 1$, we have $3u = 3v$, and so $3ij(i+j)u = 0$. Taking $i = j = 1$, we have $6u = 6v = 0$. Conversely, if $6u = 0$, then since $ij(i+j)$ is always even, $3ij(i+j)u = 0$, and so if $3u = 3v$, then $3ij(iu+jv) = 0$ for all i, j. Therefore f is PACC-good by Lemma 7.6.

Finally, note that $\mathcal{A}_f(6a, ka+\ell b, pa+qb) = -6(kq+lp)u - 6(lq)v = 0$, and so $6a \in N(P)$, and similarly $6b \in N(P)$. □

We now consider special cases of this construction.

Corollary 7.10. *Let G be an abelian group and $A = \langle a \rangle \times \langle b \rangle \cong \mathbb{Z} \times \mathbb{Z}$. Define f as in $(*2)$, and let $P = A \ltimes_f G$. Then TFAE:*

1. *For every choice of $z, u, v \in G$, P is a PACC-loop.*
2. *G is of exponent 3.*

Proof. For (1) $\implies$ (2), applying the theorem with $v = 2u$ gives $3v = 0$ for all $v \in G$. The converse is clear. □

The other special case of Theorem 7.9 we will consider is motivated by Lemma 5.7.

Corollary 7.11. *Let G be an abelian group and $A = \langle a \rangle \times \langle b \rangle \cong \mathbb{Z} \times \mathbb{Z}$. Fix $z \in G$, set $v = 2z$, $u = -2z$, and define f as in $(*2)$. Let $P = A \ltimes_f G$. Then P is a PACC-loop iff the order of z divides 12.*

Proof. In this case, $\mathcal{A}_f(ia+jb, ia+jb, ia+jb) = -3ij(iu+jv) = 6ij(i-j)z$. Since $ij(i-j)$ is always even, P is power-associative iff $12z = 0$ by Lemma 7.6. □

We now apply the corollaries to get examples with a, b of finite order:

Lemma 7.12. *Let $(G, \cdot)$ be an abelian group of exponent 3, and fix $z, u, v, t, w \in G$. Then there is a PACC-loop $Q = \langle G \cup \{a, b\} \rangle$ with $G \le Z(Q)$ and $Q/G \cong \mathbb{Z}_3 \times \mathbb{Z}_3$, such that Q satisfies:*

$$ba = abz \qquad (b)E_a = bu \qquad (a)E_b = av \qquad a^3 = t \qquad b^3 = w \quad .$$

Proof. Start with the loop $P = (\mathbb{Z} \times \mathbb{Z}) \ltimes_f G$ constructed in Theorem 7.9, where a, b have infinite order. Then $(b,0)(a,0) = (a,0)(b,0)(0,z)$, $(b,0)E_{(a,0)} = (b,0)(0,u)$, and $(a,0)E_{(b,0)} = (a,0)(0,v)$ by Lemma 7.1. Since G has exponent 3, $(*2)$ yields

$$f(ia+jb, ka+\ell b) = (-jk^2 + i\ell k + jk)u + (kj^2 - ij\ell - jk)v + (jk)z \quad . \qquad (*3)$$

Also note:

$$f(3ia + 3jb, ka + \ell b) = f(ia + jb, 3ka + 3\ell b) = 0 \quad ,$$

so that all $(3ia+3jb, x) \in Z(P)$ by Lemma 7.5. Let $H = \{(3ia+3jb, -it-jw) : i, j \in \mathbb{Z}\}$. Then $H \le Z(P)$, so H is a normal subloop, and the lemma is satisfied by P/H. To see this, note that $f(ia, ka) = f(jb, \ell b) = 0$, so that $(a, 0)^3 = (3a, 0) \equiv (0, t) \pmod H$ and $(b, 0)^3 = (3b, 0) \equiv (0, w) \pmod H$. □

When $|G| = 3$, this lemma lists all PACC-loops of order 27; see §9.

Lemma 7.13. *Let $(G, \cdot)$ be an abelian group, and fix $z, t, w \in G$ with $z^4 = 1$. Then there is a PACC-loop $Q = \langle G \cup \{a, b\}\rangle$ with $G \le Z(Q)$ and $Q/G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, such that Q satisfies:*

$$ba = abz \qquad (b)E_a = bz^{-2} \qquad (a)E_b = az^2 \qquad a^2 = t \qquad b^2 = w \quad .$$

Proof. Start with the loop $P = (\mathbb{Z}\times\mathbb{Z}) \ltimes_f G$ constructed in Theorem 7.9, where a, b have infinite order. Then $(b, 0)(a, 0) = (a, 0)(b, 0)(0, z)$, $(b, 0)E_{(a,0)} = (b, 0)(0, -2z)$, and $(a, 0)E_{(b,0)} = (a, 0)(0, 2z)$ by Lemma 7.1. Since $4z = 0$, $(*2)$ yields

$$f(ia + jb, ka + \ell b) = (2ik\ell + 2ij\ell - jk^2 - kj^2 - jk)z \quad .$$

Also note:

$$f(2ia + 2jb, ka + \ell b) = f(ia + jb, 2ka + 2\ell b) = 0 \quad ,$$

since $jk^2 + jk$ and $kj^2 + jk$ are always even; thus all $(2ia + 2jb, x) \in Z(P)$ by Lemma 7.5. Let $H = \{(2ia + 2jb, -it - jw) : i, j \in \mathbb{Z}\}$. Then $H \le Z(P)$, so H is a normal subloop, and the lemma is satisfied by P/H. □

When $G = \mathbb{Z}_4$, this lemma describes the two PACC-loops Q of order 16 with $Z(Q) = N(Q) \cong \mathbb{Z}_4$; see §8.

We conclude this section by considering the automorphic inverse property.

Definition 7.14. *A PACC-loop has the automorphic inverse property (AIP) iff the map $x \to x^{-1}$ is an automorphism.*

When $A \ltimes_f G$ is power-associative, $f(a, -a) = f(-a, a)$ for all a (see Lemma 7.6), and $(a, x)^{-1} = (-a, -x - f(a, -a))$. Then,

$$\begin{aligned}((a, x) \cdot (b, y))^{-1} &= (-a - b, -x - y - f(a, b) - f(a + b, -a - b)) \\ (a, x)^{-1} \cdot (b, y)^{-1} &= (-a - b, -x - y + f(-a, -b) - f(a, -a) - f(b, -b)) \quad ,\end{aligned}$$

so $A \ltimes_f G$ satisfies the AIP iff

$$f(a + b, -a - b) = f(a, -a) + f(b, -b) - f(-a, -b) - f(a, b)$$

holds for all $a, b \in A$. We remark that when f is bilinear, this reduces to $f(b, a) = f(a, b)$ which is equivalent to the group $A \ltimes_f G$ being abelian. Replacing a by $ia + jb$

and b by $ka + \ell b$, we get

$$\begin{gathered} f(ia + jb + ka + \ell b, -(ia + jb + ka + \ell b)) = \\ f(ia + jb, -(ia + jb)) + f(ka + \ell b, -(ka + \ell b)) \\ -f(-(ia + jb), -(ka + \ell b)) - f(ia + jb, ka + \ell b) \end{gathered}$$

Now, consider the case where G has exponent 3 and f is as in $(*3)$. Then

$$f(ia+jb, -(ia+jb)) = (-ji^2+iji-ji)u+(-ij^2+ijj+ji)v-(ji)z = -ij(u-v+z) \ .$$

So, the requirement becomes

$$\begin{aligned} &-(i+k)(j+\ell)(u-v+z) = \\ &-ij(u+v+z) - k\ell(u-v+z) \\ &-[(jk^2 - i\ell k + jk)u + (-kj^2 + ij\ell - jk)v + (jk)z] \\ &-[(-jk^2 + i\ell k + jk)u + (kj^2 - ij\ell - jk)v + (jk)z] \ . \end{aligned}$$

This simplifies to

$$(i\ell + kj)(u - v + z) = 2jk(u - v + z)$$

for all i, j, k, ℓ, which is equivalent to $v = u + z$. Passing to the quotient, we get

Lemma 7.15. *If Q is the loop constructed in Lemma 7.12, then Q has the AIP iff $v = u + z$.*

Proof. We had $Q = P/H$, where $P = (\mathbb{Z}\times\mathbb{Z})\ltimes_f G$. We have just seen that $v = u+z$ implies the AIP of P, and hence of P/H. Conversely, if $v \neq u+z$, then the AIP fails in P, with $[(ia+jb, 0)\cdot(ka+\ell b, 0)]^{-1} \setminus [(ia+jb, 0)^{-1}\cdot(ka+\ell b, 0)^{-1}] = (0, z) \neq (0, 0)$ for some i, j, k, ℓ. Since $(0, z) \notin H$, the AIP fails in Q as well. $\square$

This lemma will be used in §9 to determine which of the PACC-loops of order 27 satisfy the AIP.

8. 2-Loops

In this section we show that there are eight nonassociative PACC-loops of order 16; this includes the five extra loops already described by Chein ([5], p. 49). If Q is such a loop, then $Z = Z(Q)$ is nontrivial, so our strategy is to analyze the various possibilities for Z and N.

Lemma 8.1. *If Q is a PACC-loop of finite order 2^n, then*

1. $|Z(Q)| = 2^r$, *where* $0 < r \leq n$.
2. *Q has WIP.*
3. *$Q/N(Q)$ is an elementary abelian 2-group.*

Proof. (1) is from [17], Cor. 3.5, and is true of all CC-loops. (2) is by Corollary 3.7. (3) is by Lemma 4.18. $\square$

The five nonassociative extra loops of order 16 all have $Z(Q) = N(Q) \cong \mathbb{Z}_2$ and Q/Z an elementary abelian 2-group. For the nonextra ones, we have two cases, described by:

Lemma 8.2. *If Q is a nonextra PACC-loop of order 16, then $|N| = 4$, $Q/N \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, and either:*

1. $|Z| = 4$ *and* $Z \cong \mathbb{Z}_4$, *or*
2. $|Z| = 2$ *and* $|N| = 4$.

Proof. $|N| = 2$ or $|N| = 4$ by Corollary 5.2, but $|N| = 2$ would contradict Corollary 5.8, which also yields $|Z| = 4 \to Z \cong \mathbb{Z}_4$. $\square$

In Case (1), fix $a, b \in Q$ with $aZ \neq bZ$. Then $Q/Z = \{Z, aZ, bZ, abZ\}$. Define $z = [b, a] = (ab)\backslash(ba)$ as in Lemmas 5.5 and 5.7. Then $z^2 \neq 1$, since otherwise $\{a, b\}$ would associate, but then Q would be a group by Lemma 5.1. So, z is a generator of Z. Say $a^2 = z^r$ and $b^2 = z^s$, where $r, s \in \{0, 1, 2, 3\}$. Then, applying Lemmas 5.3 and 5.7, we get the loop $Q_{r,s}$ defined by the table:

$Q_{r,s}$	z^j	az^j	bz^j	abz^j
z^i	z^{i+j}	az^{i+j}	bz^{i+j}	abz^{i+j}
az^i	az^{i+j}	z^{i+j+r}	abz^{i+j}	$bz^{i+j+r+2}$
bz^i	bz^{i+j}	abz^{i+j+1}	z^{i+j+s}	$az^{i+j+s+1}$
abz^i	abz^{i+j}	$bz^{i+j+r+1}$	$az^{i+j+s+2}$	$z^{i+j+r+s+1}$

Each $Q_{r,s}$ really defines a PACC-loop by Lemma 7.13. $Q_{r,s}$ is never diassociative, since $aa \cdot b \neq a \cdot ab$. There are 16 possibilities for r, s, but up to isomorphism, there are only two loops, $Q_{0,0}$ and $Q_{1,1}$:

If r, s are both even, then $Q_{r,s} \cong Q_{0,0}$, since if we let $2i = -r$ and $2j = -s$ and define $\hat{a} = az^i$ and $\hat{b} = bz^j$, then $(\hat{a})^2 = (\hat{b})^2 = 1$ and $(\hat{a}\hat{b})\backslash(\hat{b}\hat{a}) = z$. If we replace a, b by $\hat{a}, \hat{b}$, we get the table for $Q_{0,0}$.

Also, if r is even and s is odd, then $Q_{r,s} \cong Q_{0,0}$. To see this, let $2i = -r$ and $2j = -r - s - 1$, and let $\hat{a} = az^i$ and $\hat{b} = abz^j$. Then $(\hat{a})^2 = (\hat{b})^2 = 1$ and $(\hat{a}\hat{b})\backslash(\hat{b}\hat{a}) = (a \cdot ab)\backslash(ab \cdot a) = \hat{z} := z^{-1}$. Replacing a, b, z by $\hat{a}, \hat{b}, \hat{z}$, we again get the table for $Q_{0,0}$.

Likewise, if r is odd and s is even, then $Q_{r,s} \cong Q_{0,0}$.

Finally, if r, s are both odd, then $Q_{r,s} \cong Q_{1,1}$, since we may let $2i = -r + 1$ and $2j = -s + 1$ and define $\hat{a} = az^i$ and $\hat{b} = bz^j$; then $(\hat{a})^2 = (\hat{b})^2 = z^1$, so that we get the table for $Q_{1,1}$.

$Q_{0,0}$ and $Q_{1,1}$ are not isomorphic, since $\{x : x^2 = 1\}$ has size 2 in $Q_{1,1}$ (namely, $\{1, z^2\}$), and size 6 in $Q_{0,0}$ (namely, $\{1, z^2, a, az^2, b, bz^2\}$).

The loops $Q_{r,s}$ are isomorphic to loop structures defined on $\mathbb{Z}_4\times\mathbb{Z}_2\times\mathbb{Z}_2$ as follows:

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} := \begin{pmatrix} x_1 + y_1 + rx_2y_2 + sx_3y_3 + 2x_2x_3y_3 + 2x_2y_2y_3 + x_3y_2^2 \\ x_2 + y_2 \\ x_3 + y_3 \end{pmatrix} .$$

The isomorphism is given on generators by $z \leftrightarrow (1,0,0)^t$, $a \leftrightarrow (0,1,0)^t$, and $b \leftrightarrow (0,0,1)^t$. The explicit formula was found by making an *ansatz* that the $\mathbb{Z}_4$-component has the form $x_1 + y_1 + rx_2y_2 + sx_3y_3 + f(x_2,x_3,y_2,y_3)$, and then computing the sixteen values of f using the table. Assuming further that f is a homogeneous cubic polynomial of the form $f(x_2,x_3,y_2,y_3) = \sum_{0\le i\le j\le k\le 1} \alpha_{ijk}x_ix_jy_k + \sum_{0\le l\le m\le n\le 1} \beta_{lmn}x_ly_my_n$ leads to a system of nine linear equations with twelve unknowns in $\mathbb{Z}_2$, namely the coefficients α_{ijk} and β_{lmn}. The particular f chosen here, namely $f(x_1,x_2,y_1,y_2) = 2x_2x_3y_3+2x_2y_2y_3+x_3y_2^2$, maximizes (though not uniquely) the number of zero coefficients.

Next, we consider Case (2). Let $Z = \{1,c\}$ and $N = \{1,c,u,v\}$. Let $Q = N \dot\cup Na \dot\cup Nb \dot\cup Nab$; so $N\dot\cup Na$ is an 8-element group. Since $u,v \in N\backslash Z$, WLOG $N \dot\cup Na$ is nonabelian. There are now three subcases:

2.1. $N \cong \mathbb{Z}_4$ and $N\dot\cup Na$ is the quaternion group.
2.2. $N \cong \mathbb{Z}_4$ and $N\dot\cup Na$ is dihedral.
2.3. N is an elementary abelian 2-group and $N\dot\cup Na$ is dihedral.

We shall see that Subcases (2.1) and (2.2) are impossible. Note that in all three cases, $Z(N\dot\cup Na) = \{1,c\} = Z(Q)$, and that all squares in $N\dot\cup Na$ lie in $\{1,c\}$.

By Lemma 5.10, $(a,a,b) = (a,b,b) = c$. Using LCC, we get $a\cdot ba = [(ab)/a]\cdot a^2$, so $(a\cdot ba)\cdot a = ab\cdot a^2$. Let $ab = dba$, with $d \in N$. Then, since a^2, c are central,

$$a^2db = dba^2 = dba\cdot a\cdot c = ab\cdot a\cdot c = a\cdot ba = a\cdot d^{-1}ab = ad^{-1}a\cdot b\cdot c \ \ ;$$

the last '=' used the fact that $(a,d^{-1}b,b) = (a,b,b) = c$. Thus, $a^2d = ad^{-1}ac$, so that $ada^{-1} = d^{-1}c$, so d is u or v.

This now refutes Subcase (2.1), since in the quaternions (where c is now -1), the conjugate of i by any element other than $\pm1, \pm i$ is $i^{-1} = -i$, not $-i^{-1}$. It also refutes Subcase (2.2). We shall view the dihedral group concretely as the symmetry group of the square. Here, c is rotation by $180°$, u and v are rotations by $90°$ and $270°$, and a is a reflection, so the conjugate of $d \in \{u,v\}$ by a is d^{-1}, not $d^{-1}c$.

We are now left with Subcase (2.3). Again, c is rotation by $180°$, and WLOG, u is reflection on the y axis, v is reflection on the x axis, and a is reflection on the line $x = y$. Then $a^2 = 1$, and we can assume WLOG that $d = u$, so $ab = uba$. Furthermore, if b,u commute then ab,u do not commute. Replacing b by ab, we may assume WLOG, that b,u do not commute so that $N\dot\cup Nb$ is nonabelian, and is thus dihedral, as we have just seen. Since some element of Nb has order 2, we may assume WLOG that $b^2 = 1$. In the dihedral group $N\dot\cup Nb$, all commutators are 1 or c, so that $ub = cbu$; it follows that u (and also v) commute with ab. We now can compute a complete table of Q; see Table 2. This table can mostly be filled out

Q	1	c	u	v	a	ca	ua	va	b	cb	ub	vb	ab	cab	uab	vab
1	1	c	u	v	a	ca	ua	va	b	cb	ub	vb	ab	cab	uab	vab
c	c	1	v	u	ca	a	va	ua	cb	b	vb	ub	cab	ab	vab	uab
u	u	v	1	c	ua	va	a	ca	ub	vb	b	cb	uab	vab	ab	cab
v	v	u	c	1	va	ua	ca	a	vb	ub	cb	b	vab	uab	cab	ab
a	a	ca	va	ua	1	c	v	u	ab	cab	vab	uab	cb	b	ub	vb
ca	ca	a	ua	va	c	1	u	v	cab	ab	uab	vab	b	cb	vb	ub
ua	ua	va	ca	a	u	v	c	1	uab	vab	cab	ab	vb	ub	b	cb
va	va	ua	a	ca	v	u	1	c	vab	uab	ab	cab	ub	vb	cb	b
b	b	cb	vb	ub	uab	vab	cab	ab	1	c	v	u	ua	va	ca	a
cb	cb	b	ub	vb	vab	uab	ab	cab	c	1	u	v	va	ua	a	ca
ub	ub	vb	cb	b	ab	cab	vab	uab	u	v	c	1	a	ca	va	ua
vb	vb	ub	b	cb	cab	ab	uab	vab	v	u	1	c	ca	a	ua	va
ab	ab	cab	uab	vab	vb	ub	cb	b	ca	a	va	ua	v	u	c	1
cab	cab	ab	vab	uab	ub	vb	b	cb	a	ca	ua	va	u	v	1	c
uab	uab	vab	ab	cab	cb	b	vb	ub	va	ua	ca	a	c	1	v	u
vab	vab	uab	cab	ab	b	cb	ub	vb	ua	va	a	ca	1	c	u	v

TABLE 2. Subcase (2.3)

using the commutation and association relations already described. To fill out the lower right 4×4, we need to know that $ab \cdot ab = v$. To see that, use LCC to get $ab \cdot ab = [(ab \cdot a)/(ab)] \cdot (ab \cdot b)$. But $ab \cdot a = c \cdot a \cdot ba = cau \cdot ab$, and $ab \cdot b = ca$, so that $ab \cdot ab = cau \cdot ca = aua = v$.

Thus, Case (2) of Lemma 8.2 yields just one non-extra PACC-loop of order 16. Of course, one must verify that the loop described by Table 2 really is PACC. Unlike Case (1), this does not follow by the results of Section 7; but it can easily be verified by a short computer program.

The loop of Case (2) is isomorphic to a loop structure defined on $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ as follows:

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} := \begin{pmatrix} x_1 + y_1 + x_3 y_2 + x_3 y_3 y_4 + x_4 y_2^2 + x_3 x_4 (y_3 + y_4) \\ x_2 + y_2 + x_4 y_3^2 \\ x_3 + y_3 \\ x_4 + y_4 \end{pmatrix}.$$

The isomorphism is given on generators by $c \leftrightarrow (1,0,0,0)^t$, $u \leftrightarrow (0,1,0,0)^t$, $a \leftrightarrow (0,0,1,0)^t$, $b \leftrightarrow (0,0,0,1)^t$. The term x_3y_2 in the first component is determined by assuming it is quadratic in the variables, and then using the equation $au = va$ in the dihedral group $N\dot{\cup}Na$, the upper left 8×8 corner of the table. Analogously to Case (1), the remaining terms in the first and second components were found by assuming that they are homogeneous cubic polynomials in $x_2, x_3, x_4, y_2, y_3, y_4$, where each term contains at least one x_4 or y_4. Since $u \in N$, it is clear from the table that the values of the polynomials are independent of x_2. Using the table to compute values determines some coefficients; the choice above maximizes (though not uniquely) the number of zero coefficients.

9. Order 27

Q	1	a	a^2	b	ab	a^2b	b^2	ab^2	a^2b^2	cubes
1	0	0	0	0	0	0	0	0	0	0
a	0	0	α	0	γ	$\alpha+2\gamma$	0	2γ	$\alpha+\gamma$	α
a^2	0	α	α	0	$\alpha+2\gamma$	$\alpha+\gamma$	0	$\alpha+\gamma$	$\alpha+2\gamma$	2α
b	0	θ	$2\theta+\gamma$	0	θ	$2\theta+\gamma$	β	$\theta+\beta$	$2\theta+\beta+\gamma$	β
ab	0	θ	$2\theta+\alpha+\gamma$	2δ	$\theta+\gamma+2\delta$	$2\theta+\alpha+2\delta$	$\beta+\delta$	$\theta+\beta+2\gamma+\delta$	$2\theta+\alpha+\beta+2\gamma+\delta$	$\alpha+\beta$
a^2b	0	$\theta+\alpha$	$2\theta+\alpha+\gamma$	δ	$\theta+\alpha+2\gamma+\delta$	$2\theta+\alpha+2\gamma+\delta$	$\beta+2\delta$	$\theta+\alpha+\beta+\gamma+2\delta$	$2\theta+\alpha+\beta+2\delta$	$2\alpha+\beta$
b^2	0	$2\theta+2\delta$	$\theta+2\gamma+\delta$	β	$2\theta+\beta+2\delta$	$\theta+\beta+2\gamma+\delta$	β	$2\theta+\beta+2\delta$	$\theta+\beta+2\gamma+\delta$	2β
ab^2	0	$2\theta+2\delta$	$\theta+\alpha+2\gamma+\delta$	$\beta+\delta$	$2\theta+\beta+\gamma$	$\theta+\alpha+\beta+\gamma+2\delta$	$\beta+2\delta$	$2\theta+\beta+2\gamma+\delta$	$\theta+\alpha+\beta$	$\alpha+2\beta$
a^2b^2	0	$2\theta+\alpha+2\delta$	$\theta+\alpha+2\gamma+\delta$	$\beta+2\delta$	$2\theta+\alpha+\beta+2\gamma+\delta$	$\theta+\alpha+\beta$	$\beta+\delta$	$2\theta+\alpha+\beta+\gamma$	$\theta+\alpha+\beta+\gamma+2\delta$	$2\alpha+2\beta$

Table 3. Order 27

If Q is a nonassociative PACC-loop of order 27, then $|N(Q)| = |Z(Q)| = 3$, and Q/N is an abelian group of exponent 3. Thus Q is an *extraspecial* CC-loop, and one may then in principle use Drápal's description of all extraspecial CC-loops to classify the PACC-loops of order 27; see §7 of [11]. Here we adopt a direct approach based on Lemmas 5.5 and 7.12.

Say $N = \{1, n, n^2\}$ and Q/N has generators Na, Nb. Then Q is determined by five parameters, $\theta, \alpha, \beta, \gamma, \delta \in \mathbb{Z}_3 = \{0, 1, 2\}$, where $ba = abn^\theta$, $a^3 = n^\alpha$, $b^3 = n^\beta$, $(b)E_a = bn^\gamma$, and $(a)E_b = an^\delta$. Then $a^ib^j \cdot a^kb^\ell = a^{i+k}b^{j+\ell}n^{f(i,j,k,\ell)}$, and Table 3 displays $f(i,j,k,\ell)$. Likewise, $(a^ib^j)^3 = n^{g(i,j)}$, and the table displays $g(i,j)$. The table is computed using Lemma 5.5, and the loop is PACC by Lemma 7.12.

We now count the number of distinct PACC-loops we have.

Let $T = \{x \in Q : x^3 = 1\}$. By inspection of the table, we see that T is always a subloop of order either 9 or 27.

Next, let $M = M(Q) = \{x \in Q : E_x = I\}$, the set of Moufang elements of Q. Clearly $N \subseteq M \subseteq Q$. In fact, $N \subsetneqq M \subsetneqq Q$. First, $M \neq Q$: Q cannot be Moufang because it is not even WIP by Theorem 6.4 (or, by Chein [5], a Moufang loop of order 27 is a group). Now, suppose that $M = N$. Then $\gamma, \delta \in \{1, 2\}$, so that $\gamma = \pm\delta$. Referring to the table, we see:

$$(a \cdot ab) \cdot ab = a^2b \cdot ab \cdot n^\gamma = a^3b^2 \cdot n^{\theta+\alpha+\delta} = b^2 \cdot n^{\theta+2\alpha+\delta} \quad .$$
$$a \cdot (ab)^2 = a \cdot a^2b^2 \cdot n^{\theta+\gamma+2\delta} = a^3b^2 \cdot n^{\theta+\alpha+2\gamma+2\delta} = b^2 \cdot n^{\theta+2\alpha+2\gamma+2\delta} \quad .$$
$$(a \cdot a^2b) \cdot a^2b = a^3b \cdot a^2b \cdot n^{\alpha+2\gamma} = b \cdot a^2b \cdot n^{2\alpha+2\gamma} = a^2b^2 \cdot n^{2\theta+2\alpha} \quad .$$
$$a \cdot (a^2b)^2 = a \cdot a^4b^2 \cdot n^{2\theta+\alpha+2\gamma+\delta} = a \cdot ab^2 \cdot n^{2\theta+2\alpha+2\gamma+\delta} = a^2b^2 \cdot n^{2\theta+2\alpha+\gamma+\delta} \quad .$$

If $\gamma = \delta$, then $(a \cdot ab) \cdot ab = a \cdot (ab)^2$, so $(a)E_{ab} = a$ (using $tx \cdot x = tx^2 \to tE_x = t$ by RAlt= RIP from Lemma 4.1). Since also $(ab)E_{ab} = ab$, we have $E_{ab} = I$, contradicting $M = N$. Likewise, if $\gamma = -\delta$, then $(a \cdot a^2b) \cdot a^2b = a \cdot (a^2b)^2$, which implies $E_{a^2b} = I$, again a contradiction.

As we noted in Conjecture 4.8, we do not think that for arbitrary PACC-loops, the set of Moufang elements is necessarily a subloop. However, for this particular loop, M is indeed a subloop of order 9. To see this, use $M \neq N$, and choose a generator a such that $E_a = I$ (that is, $\gamma = 0$). Then $E_{a^2} = E_a^4 = I$, so $M \supseteq N \cup Na \cup Na^2$. If $|M| > 9$, then we could choose the other generator b so that $E_b = I$; but then $\delta = 0$, and then, as above, all $E_x = I$, so that $M = Q$, which is false.

Thus, $|M| = 9$, and as noted, we shall always choose our generators so that $M = N \cup Na \cup Na^2$, and so $\gamma = 0$ and $\delta \in \{1, 2\}$. Since $N = Z$, this shows that M is a subloop. We now have three cases:

I. $T = Q$.
II. $T = M$.
III. $|T| = 9$ and $T \neq M$.

Furthermore, each case will split into two subcases:

A. $\exists x \in Q \backslash M \; \exists y \in M \backslash N \; [xy = yx]$.
B. $\forall x \in Q \backslash M \; \forall y \in M \backslash N \; [xy \neq yx]$.

In Case I, we have $\alpha = \beta = \gamma = 0$, and the generator b can be any element outside of M. In Case IA, we can choose a and b so that a, b commute, so that $\theta = 0$. Then, WLOG $\delta = 1$, since we can always replace n by n^2. In Case IB, we see from Table 3 that $\theta \neq 0$ and $\theta + \delta \neq 0$ (in $\mathbb{Z}_3$), so that $\theta = \delta \in \{1, 2\}$. Again, replacing n by n^2, we may assume WLOG that $\theta = \delta = 1$. Thus, Case I yields two loops.

In Case II, we have $T = M = N \cup Na \cup Na^2$, so that $\alpha = \gamma = 0$ and $\beta, \delta \in \{1, 2\}$.

In Case IIA, we can choose $a \in M \backslash N$ and $b \in Q \backslash M$, so that $ab = ba$; so $\theta = 0$. Now $b^3 = n^\beta$, but replacing n by n^2 if necessary, WLOG $\beta = 1$. Also, $(a)E_b = an^\delta$, so $(a^2)E_b = a^2 n^{2\delta}$, so replacing a by a^2 if necessary, WLOG $\delta = 1$; note that by $\theta = \gamma = 0$, $ba^2 = a^2 b$, so replacing a by a^2 will not change our $\theta = 0$.

In Case IIB, note from the table that $\theta \neq 0$ and $\theta + \delta \neq 0$ (in $\mathbb{Z}_3$). WLOG $\theta = 1$, so that also $\delta = 1$; that is, we choose b, n so that $ba = abn$. From the table, $b^2 a = ab^2 n$. Also $(b^2)^3 = n^{2\beta}$. Thus, replacing b by b^2 if necessary, WLOG $\beta = 1$.

Thus, Case II yields two loops.

In Case III, we may choose generators so that $M = N \cup Na \cup Na^2$ and $T = N \cup Nb \cup Nb^2$. Then $\beta = \gamma = 0$ and $\alpha, \delta \in \{1, 2\}$.

Now Case IIIA splits into two subcases:

1. $\exists x \in T \backslash N \; \exists y \in M \backslash N \; [xy = yx]$.
2. $\forall x \in T \backslash N \; \forall y \in M \backslash N \; [xy \neq yx]$.

In case IIIA1, WLOG $\theta = 0$. Then b commutes with both of a, a^2, whereas b^2 commutes with neither of a, a^2, so b is fixed. WLOG $\alpha = 1$; that is, we choose a, n so that $a^3 = n$; then also a^2, n^2 satisfy $(a^2)^3 = n^2$. Now $\delta \in \{1, 2\}$ is determined by $(a)E_b = (a)n^\delta$; then $(a^2)E_b = (a^2)(n^2)^\delta$. Thus, δ is determined from the loop structure, so that we have two distinct loops. In Case IIIA2, WLOG $\theta = 1$. Then also $\delta = 1$, since otherwise b^2 would commute with a. But then regardless of the choice of α, neither of a, a^2 commute with any element of $\{b, ab, a^2 b, b^2, ab^2, a^2 b^2\}$, contradicting the assumption in IIIA.

In Case IIIB, WLOG $\theta = 1$; so $[b, a]$ is n, not n^2. Then, as in Case IIIA2, we need $\delta = 1$, and this guarantees that we are in IIIB for either choice of $\alpha \in \{1, 2\}$. For each choice, we have $\forall x \in M \backslash N \, \forall y \in T \backslash N \, [\, [y, x] = x^{3\alpha} \,]$, so there are two distinct loops here.

Thus, Case III yields four loops, and there are exactly eight nonassociative PACC-loops of order 27. By Lemma 7.15, the AIP holds in one if these loops iff $\delta = \gamma + \theta$. Since our loops all had $\gamma = 0$, we need $\delta = \theta$, which is true of the four "B" loops and false of the four "A" loops; so there are exactly four nonassociative AIP PACC-loops of order 27.

References

[1] А. С. Басараб, Об одном классе G-луп, *Математические Исследования* Том 3, Вып. 2 (8) (1968) 72–77.

[2] А. С. Басараб, Класс LK-луп, *Математические Исследования* Вып. 120 (1991) 3–7. MR 92g:20115.

[3] В. Д. Белоусов, *Основы Теории Квазигрупп и Луп*, Издательство «Наука», Москва, 1967. MR 36#1569, Zbl 163.01801.

[4] R. H. Bruck, *A Survey of Binary Systems*, Springer-Verlag, 1971. MR 20#76, Zbl 206.30301.

[5] O. Chein, Moufang loops of small order, I, *Trans. Amer. Math. Soc.* **188** (1974) 31–51. MR 48#8673, Zbl 286.20088.
[6] O. Chein, H. O. Pflugfelder, and J. D. H. Smith, eds., *Quasigroups and Loops: Theory and Applications* Heldermann Verlag, 1990. MR 93g:20133, Zbl 719.20036.
[7] P. Csörgő and A. Drápal, Left conjugacy closed loops of nilpotency class 2, preprint.
[8] A. Drápal, Conjugacy closed loops and their multiplication groups, *J. Algebra* **272** (2004), 838–850.
[9] A. Drápal, Structural interactions of conjugacy closed loops, preprint.
[10] A. Drápal, On multiplication groups of left conjugacy closed loops, *Comment. Math. Univ. Carolinae* **45** (2004) 191–212.
[11] A. Drápal, On extraspecial left conjugacy closed loops, preprint.
[12] F. Fenyves, Extra loops I, *Publ. Math. Debrecen* **15** (1968) 235–238. MR 38#5976, Zbl 172.02401.
[13] F. Fenyves, Extra loops II, *Publ. Math. Debrecen* **16** (1969) 187–192. MR 41#7017, Zbl 221.20097.
[14] E. G. Goodaire and D. A. Robinson, A class of loops which are isomorphic to all loop isotopes, *Canadian J. Math.* **34** (1982) 662–672. MR 83k:20079, Zbl 467.20052.
[15] E. G. Goodaire and D. A. Robinson, Some special conjugacy closed loops, *Canadian Math. Bull.* **33** (1990) 73–78. MR 91a:20077, Zbl 661.20046.
[16] M. K. Kinyon and K. Kunen, The structure of extra loops, *Quasigroups and Related Systems* **12** (2004) 39–60.
[17] M. K. Kinyon, K. Kunen, and J. D. Phillips, Diassociativity in conjugacy closed loops, *Comm. Algebra* **32** (2004) 767–786.
[18] K. Kunen, The structure of conjugacy closed loops, *Trans. Amer. Math. Soc.* **352** (2000) 2889–2911. MR 2000j:20132, Zbl 962.20048.
[19] W. W. McCune, *Mace 4.0 Reference Manual and Guide*, Argonne National Laboratory Technical Memorandum ANL/MCS-TM-264, 2003; `http://www.mcs.anl.gov/AR/mace4/`
[20] W. W. McCune, *OTTER 3.3 Reference Manual and Guide*, Argonne National Laboratory Technical Memorandum ANL/MCS-TM-263, 2003; `http://www.mcs.anl.gov/AR/otter/`
[21] P. T. Nagy and K. Strambach, Loops as invariant sections in groups, and their geometry, *Canad. J. Math.* **46** (1994) 1027–1056. MR 95h:20088, Zbl 814.20055.
[22] H. O. Pflugfelder, *Quasigroups and Loops: Introduction*, Sigma Series in Pure Math. **8**, Heldermann Verlag, Berlin, 1990. MR 93g:20132, Zbl 719.20036.
[23] Л. Р. Сойкис, О Специальных лупах, in *Вопросы Теории Квазигрупп и Луп* (В. Д. Белоусов, ed.), Редакц.-Издат. Отдел Акад. Наук Молдав. ССР, Кишинев, 1970, pp. 122–131.

Department of Mathematical Sciences, Indiana University South Bend, South Bend, IN 46634 USA
E-mail address: `mkinyon@iusb.edu`
URL: `http://mypage.iusb.edu/~mkinyon`

Department of Mathematics, University of Wisconsin, Madison, WI 57306 USA
E-mail address: `kunen@math.wisc.edu`
URL: `http://www.math.wisc.edu/~kunen`