C-LOOPS: EXTENSIONS AND CONSTRUCTIONS

MICHAEL K. KINYON, J. D. PHILLIPS, AND PETR VOJTĚCHOVSKÝ

ABSTRACT. C-loops are loops satisfying the identity $x(y \cdot yz) = (xy \cdot y)z$. We develop the theory of extensions of C-loops, and characterize all nuclear extensions provided the nucleus is an abelian group. C-loops with central squares have very transparent extensions; they can be built from small blocks arising from the underlying Steiner triple system. Using these extensions, we decide for which abelian groups K and Steiner loops Q there is a nonflexible C-loop C with center K such that C/K is isomorphic to Q. We discuss possible orders of associators in C-loops. Finally, we show that the loops of signed basis elements in the standard real Cayley-Dickson algebras are C-loops.

1. INTRODUCTION

This is the second paper in a series devoted to *C-loops*, which are loops satisfying the identity $x(y \cdot yz) = (xy \cdot y)z$. C-loops were introduced by Fenyves [6]. Moufang C-loops are exactly Fenyves' *extra loops* [5, 8]. The first detailed study of general C-loops was in [14]. In particular, it was observed that C-loops can be characterized as inverse property loops with all squares in the nucleus. We also examined basic loop-theoretical properties of C-loops, established some connections between C-loops, Steiner loops and commutative Moufang loops, proved a structural result for torsion commutative C-loops, and obtained the first few smallest nonextra C-loops.

In the present paper, we are concerned with constructions of C-loops. We assume some familiarity with [14], but results from there are quoted as needed. For general background in loop theory, the standard references are [1, 2, 4, 13].

In §2, we develop the theory of extensions for C-loops. Given an abelian group K and a C-loop Q we show that a C-loop C is an extension of K by Q if and only if there is a C-factor set (C-cocycle) satisfying a certain condition; see Theorem 2.4.

In §3 we consider central extensions, that is, when K is contained in the center $Z(C)$ of the C-loop extension C. For C-loops with central squares, the C-factor set condition for central extensions is greatly simplified. Moreover, the corresponding extensions can be constructed from small blocks arising from the combinatorial properties of the underlying Steiner triple system. These "block extensions" are described in §4.

If L is a C-loop with nucleus $N = N(L)$, then L/N is a Steiner loop. Furthermore, when $Z = Z(L)$ is the center of L then L/Z is Steiner if and only if every square in L is central. One of the main themes of the paper is the following question:
For which abelian groups K and Steiner loops Q is there a C-loop C with nucleus/center isomorphic to K such that C/K is isomorphic to Q?
A loop is *flexible* if it satisfies the identity $x \cdot yx = xy \cdot x$. In particular, commutative loops are flexible. Flexible C-loops are diassociative, *i.e.*, any two elements generate an

Date: December 20, 2004.
1991 *Mathematics Subject Classification.* 20N05.
Key words and phrases. C-loops, Steiner loops, Cayley-Dickson process, sedenions, loop extensions, nuclear extensions, central extensions.

associative subloop [14, Lemma 4.4]. It turns out to be easier to answer our question in the *non*flexible case. Besides, focusing on nonflexible C-loops ensures that the extension is neither Moufang nor Steiner.

When the abelian group K is the center of the nonflexible C-loop C, we answer our question completely (cf. Theorem 5.7). When K is the nucleus of C, the only unresolved case is where K is an elementary abelian 2-group, and even then we have partial results (cf. §5).

We conclude §5 with a construction that yields nonflexible C-loops that possess an associator of given order n, where $n > 2$.

Next, consider the standard Cayley-Dickson algebras over the real numbers. It is possible to choose their bases in such a way that the signed basis elements form a loop under multiplication regardless of the dimension. This is shown in §6. In fact, the loops are flexible C-loops, and if the dimension of the algebra is at least 32, then the loops are neither Moufang nor commutative, and have nucleus (and hence center) of order 2; see §7.

Conjectures and open problems are presented throughout the paper.

2. Nuclear extensions

For the general extension theory of loops, we refer the reader to [4, Chapter III]. Here we limit ourselves to C-loops. Our first goal is to characterize a broad class of extensions of C-loops. Our notation for extensions is set up to resemble that of [16].

Let K, Q be C-loops. Then a loop C is said to be an *extension of K by Q* if K is a normal subloop of C such that C/K is isomorphic to Q.

In the above situation, let $\pi : C \to C/K = Q$ be the natural projection, and let $\ell : Q \to C$ be a *section* of π, i.e, $\pi\ell x = x$ for every $x \in Q$. Throughout the paper, we assume that $\ell 1 = 1$ whenever ℓ is a section. Then, for $x, y \in Q$, we have $K(\ell x \cdot \ell y) = K(\ell(xy))$, and there is therefore a unique element $f(x, y) \in K$ such that

$$\ell x \cdot \ell y = f(x, y) \cdot \ell(xy).$$

The resulting map $f : Q \times Q \to K$ is said to be *associated with* ℓ.

Let $\theta : Q \to \operatorname{Aut} K; x \mapsto \theta_x$ be a homomorphism. The pair (θ, f) is said to be a *C-factor set* (or *C-cocycle*) if

$$f(x, 1) = 1 = f(1, x), \tag{1}$$

and

$$\theta_{xy} f(y, z) \cdot \theta_x f(y, yz) \cdot f(x, y \cdot yz) = f(x, y) \cdot f(xy, y) \cdot f(xy \cdot y, z) \tag{2}$$

holds for every x, y, $z \in Q$.

Remark 2.1. Equation (2) is ambiguous unless K is associative. In all situations discussed below, K is an abelian group. A less general notion of a C-factor set (with trivial θ) was introduced in [14].

Given a C-factor set (θ, f), we define a binary operation $*$ on $D = K \times Q$ by

$$(a, x) * (b, y) = (a \cdot \theta_x b \cdot f(x, y),\ xy), \tag{3}$$

for $a, b \in K$ and $x, y \in Q$. We denote the resulting quasigroup by $K \ltimes_\theta^f Q$.

For a loop C and $x \in C$, we denote the left and right multiplication maps by $L_x : C \to C; y \mapsto xy$ and $R_x : C \to C; y \mapsto yx$, respectively. Set $T_x = R_x^{-1} L_x$; these are usually called *middle inner mappings*. In group theory, T_x is conjugation by x, and is an automorphism. This is not necessarily so when C is not associative. Roughly speaking, the theory of extensions of loops can imitate the theory of extensions of groups so long

as the middle inner mappings T_x behave as automorphisms on the normal subloops in question, and satisfy $T_xT_y = T_{xy}$.

Since every C-loop is an inverse property loop ([14, Corollary 2.4]), we have $T_x = R_{x^{-1}}L_x$.

Proposition 2.2. *Let K be an abelian group, Q a C-loop, $f : Q \times Q \to K$ a map, and $\theta : Q \to \operatorname{Aut} K$ a homomorphism. Then $D = K \ltimes_\theta^f Q$ is a C-loop with neutral element $(1, 1)$ if and only if (θ, f) is a C-factor set. Moreover, when D is a C-loop, we have:*

(i) $K \cong (K, 1) \le D$, $Q \cong (1, Q) \le D$,
(ii) $K \le N(D)$,
(iii) *for every* $a \in K$, $x \in Q$, $(a, x)^{-1} = (\theta_x(f(x, x^{-1})a),\ x^{-1})$,
(iv) *for every* $a \in K$, $x \in Q$, $\theta_x = T_{(a,x)}|_K$,
(v) $K \trianglelefteq D$, $D/K \cong Q$.

Proof. Let $u = (a, x)$, $v = (b, y)$, $w = (c, z)$, for a, b, $c \in K$, x, y, $z \in Q$. Then

$$\begin{aligned} u * (v * (v * w)) &= u * (v * (b\theta_y cf(y, z),\ yz)) \\ &= u * (b\theta_y(b\theta_y cf(y, z))f(y, yz),\ y \cdot yz) \\ &= (a\theta_x(b\theta_y(b\theta_y cf(y, z))f(y, yz))f(x, y \cdot yz),\ x(y \cdot yz)) \\ &= (a\theta_x b\theta_{xy} b\theta_{xy\cdot y} c\theta_{xy} f(y, z)\theta_x f(y, yz)f(x, y \cdot yz),\ x(y \cdot yz)). \end{aligned}$$

On the other hand

$$\begin{aligned} ((u * v) * v) * w &= ((a\theta_x bf(x, y),\ xy) * v) * w \\ &= (a\theta_x bf(x, y)\theta_{xy} bf(xy, y),\ xy \cdot y) * w \\ &= (a\theta_x bf(x, y)\theta_{xy} bf(xy, y)\theta_{xy\cdot y} cf(xy \cdot y, z),\ (xy \cdot y)z). \end{aligned}$$

Since Q is a C-loop and K is an abelian group, we see that $u*(v*(v*w)) = ((u*v)*v)*w$ if and only if (2) holds.

We have $(a, x) * (1, 1) = (af(x, 1), x)$ and $(1, 1) * (a, x) = (af(1, x), x)$. Thus $(1, 1)$ is the neutral element of D if and only if (1) holds.

For the rest of the proof, assume that D is a C-loop. Part (i) is straightforward. For $a, b, c \in K$, $y, z \in Q$, we have $(a, 1) * ((b, y) * (c, z)) = (a, 1) * (b\theta_y cf(y, z),\ yz) = (ab\theta_y cf(y, z),\ yz) = (ab, y) * (c, z) = ((a, 1) * (b, y)) * (c, z)$. Therefore K is contained in the left nucleus of D. By [14, Corollary 2.5], the three nuclei of D coincide, and (ii) follows.

As inverse property loops, C-loops satisfy the identity $(xy)^{-1} = y^{-1}x^{-1}$. Let $(a, x) \in D$. Then

$$\begin{aligned} &(a,\ x)(\theta_x(f(x, x^{-1})a),\ x^{-1}) = (a\theta_x\theta_x(f(x, x^{-1})a)f(x, x^{-1}),\ 1) \\ &= (a\theta_x\theta_x^{-1}(a^{-1}f(x, x^{-1})^{-1})f(x, x^{-1}),\ 1) = (1,\ 1), \end{aligned}$$

proving (iii).

Upon identifying K with $(K, 1)$ and Q with $(1, Q)$, it makes sense to write $\theta_x(k, 1) = \theta_x k = (\theta_x k, 1)$ for every $k \in K$, $x \in Q$. Given $(a, x) \in D$, a short calculation yields $T_{(a,x)}(k, 1) = (a, x)(k, 1) \cdot (a, x)^{-1} = (\theta_x k, 1)$, and we are done with (iv).

In order to check that K is normal in D, we must show that K is invariant under the standard generators for the inner mapping group: $L(x, y) = L_{yx}^{-1}L_yL_x$, $R(x, y) = R_{xy}^{-1}R_yR_x$, T_x, for $x, y \in D$. Since K is nuclear, K is trivially invariant under each $L(x, y)$ and $R(x, y)$. By (iv), K is invariant under each T_x, and so $K \trianglelefteq D$ follows. It is then easy to show that K/D is isomorphic to Q. □

The following result of Leong [11, Theorem 3] is important here:

Lemma 2.3. *Let Q be a loop with a normal subloop $K \leq N(Q)$. For each $x \in Q$, define $\theta_x = T_x|_K$. Then*

(1) *For each $x \in Q$, $\theta_x \in Aut(K)$,*
(2) *The mapping $\theta : Q \to Aut(K)$ is a homomorphism.*

Proof. First fix $a, b \in K$ and $x \in Q$. Since K is normal in Q, we have $\theta_x(K) \leq K \leq N(Q)$. In particular, $T_x(ab) \cdot x = x \cdot ab = xa \cdot b = (T_x(a) \cdot x)b = T_x(a) \cdot xb = T_x(a)(T_x(b) \cdot x) = T_x(a)T_x(b) \cdot x$. Cancelling x on the right then shows that θ_x is an automorphism of K.

Now fix $a \in K$ and $x, y \in Q$. Let $z = T_{xy}a$. By the first part, $z \in K$, and so $(zx)y = z(xy) = (xy)a = x(ya) = x(T_y(a) \cdot y) = xT_y(a) \cdot y$. Upon cancelling y on the right, we get $zx = xT_y(a)$, i.e., $z = T_xT_y(a)$. Hence $\theta_{xy} = \theta_x\theta_y$ as claimed. □

Theorem 2.4. *Let K be an abelian group and Q a C-loop. The following conditions are equivalent:*

(i) *C is a C-loop extension of K by Q, and $K \leq N(C)$,*
(ii) *there is a homomorphism $\theta : Q \to \operatorname{Aut} K$ and a map $f : Q \times Q \to K$ such that (θ, f) is a C-factor set and $C = K \ltimes_\theta^f Q$.*

Proof. If (ii) holds, (i) follows by Proposition 2.2.

Conversely, assume that (i) holds. Let $\pi : C \to C/K = Q$ be the natural projection, and let $\ell : Q \to C$ be a section. Let $f : Q \times Q \to K$ be associated with ℓ. By Lemma 2.3, the map $\theta : Q \to \operatorname{Aut} K$, $x \mapsto \theta_x = T_{\ell(x)}|_K$ is well-defined. Given $x, y \in Q$, let $n = f(x, y) \in N(C)$. Then, by Lemma 2.3, $\theta_x\theta_y = T_{n\ell(xy)} = T_n\theta_{xy} = \theta_{xy}$, showing that θ is a homomorphism. We proceed to show that (θ, f) is a C-factor set.

Let $x, y, z \in Q$. On the one hand,

$$\begin{aligned}(\ell(x)\ell(y) \cdot \ell(y))\ell(z) &= (f(x, y)\ell(xy) \cdot \ell(y))\ell(z) = f(x, y)(\ell(xy)\ell(y) \cdot \ell(z)) \\ &= f(x, y)f(xy, y)\ell(xy \cdot y)\ell(z) = f(x, y)f(xy, y)f(xy \cdot y, z)\ell((xy \cdot y)z),\end{aligned}$$

as $K \leq N(C)$. On the other hand, since C is an inverse property loop, $K \leq N(C)$ and $T_{\ell(x)}|_K = \theta_x \in \operatorname{Aut} K$, we have

$$\ell(x) \cdot uv = \ell(x)u \cdot v = (T_{\ell(x)}u \cdot \ell(x))v = (\theta_x u \cdot \ell(x))v = \theta_x u \cdot \ell(x)v$$

for every $u \in K$, $v \in C$, and therefore

$$\begin{aligned}&\ell(x)(\ell(y) \cdot \ell(y)\ell(z)) = \ell(x)(\ell(y) \cdot f(y, z)\ell(yz)) = \ell(x)(\theta_y f(y, z) \cdot \ell(y)\ell(yz)) \\ &= \ell(x)(\theta_y f(y, z) \cdot f(y, yz)\ell(y \cdot yz)) = \ell(x)\theta_y f(y, z) \cdot f(y, yz)\ell(y \cdot yz) \\ &= \theta_x\theta_y f(y, z) \cdot \ell(x)(f(y, yz)\ell(y \cdot yz)) = \theta_{xy} f(y, z) \cdot \theta_x f(y, yz) \cdot \ell(x)\ell(y \cdot yz) \\ &= \theta_{xy} f(y, z) \cdot \theta_x f(y, yz) \cdot f(x, y \cdot yz) \cdot \ell(x, y \cdot yz).\end{aligned}$$

As both C and Q are C-loops, we deduce that (θ, f) satisfies (2). Since (1) holds by definition of f, (θ, f) is a C-factor set.

It remains to show that there is an isomorphism ψ from C to $(D, *) = K \ltimes_\theta^f Q$. Given $u \in C$, there are uniquely determined elements $a \in K$, $x \in Q$ such that $u = ax$. Accordingly, we set $\psi(u) = (a, x)$. Then ψ is a bijection, and it suffices to prove that it is a homomorphism. Consider $v = by$ where $b \in K$, $y \in Q$. Since $a, b \in N(C)$, we have $u \cdot v = a(xb \cdot y)$, which can be rewritten as $a(\theta_x b \cdot xy) = a\theta_x b \cdot xy$, using the same trick as above. Then $\psi(u \cdot v) = (a\theta_x b,\, xy) = (a, x) * (b, y) = \psi(u) * \psi(v)$. □

Since we would like to understand the extensions of C-loops up to isomorphism, we ask:

Problem 2.5. *Let K be an abelian group, Q a C-loop, and (θ, f), (θ', f') two C-factor sets. Under which conditions on (θ, f), (θ', f') are the C-loops $K \ltimes_\theta^f Q$, $K \ltimes_{\theta'}^{f'} Q$ isomorphic?*

2.1. **C-loops with nonabelian nucleus.** Theorem 2.4 does not capture all nuclear extensions for C-loops since there are C-loops with nonabelian nucleus. For instance, let D be the direct product of the symmetric group S_3 and the smallest nonassociative Steiner loop Q of order 10. Then D is a C-loop of order 60, and the nucleus of D contains (and in fact, coincides with) S_3, a nonabelian group.

Recall the following result:

Theorem 2.6. *Let L be a nonassociative loop with normal nucleus $N = N(L)$ such that L/N is a group. Then N has nontrivial center.*

Proof. This can be found in, for instance, [9, §4]. □

Corollary 2.7. *Let C be a nonassociative C-loop with nucleus $N = N(C)$, and assume that N has trivial center. Then C/N is a nonassociative Steiner loop. In particular, $|C| \geq 10|N|$.*

Proof. The quotient C/N is a Steiner loop by [14, Proposition 5.8]. Since C is nonassociative, Theorem 2.6 implies that C/N cannot be a group. The smallest nonassociative Steiner loop has order 10. □

This shows that the above direct product is the smallest nonassociative C-loop with nucleus isomorphic to S_3. However, it is conceivable that there is a smaller C-loop with nonabelian nucleus, provided the nucleus does not have trivial center. We therefore ask:

Problem 2.8. *What is the smallest integer n for which there exists a C-loop of order n with nonabelian nucleus?*

Exhaustive computer searches suggest that there is no C-loop of order 32 with a nucleus containing a nonabelian group of order 8.

3. Central extensions

The C-loop extensions described in the previous section can, as the section's title suggests, be considered to be nuclear extensions. Not surprisingly, central C-loop extensions are characterized by the triviality of the homomorphism θ.

Lemma 3.1. *Let K be an abelian group, Q a C-loop, (θ, f) a C-factor set and $C = K \ltimes_\theta^f Q$. Then $K \leq Z(C)$ if and only if $\theta = \mathrm{id}$.*

Proof. If $\theta = \mathrm{id}$, then for every $a, b \in K$ and $x \in Q$, we have $(a,1)(b,x) = (ab,x) = (ba,x) = (b,x)(a,1)$, so that $K \leq Z(C)$.

Conversely, if $K \leq Z(C)$, then $(a,1)(b,x) = (ab,x)$ is equal to $(b,x)(a,1) = (b\theta_x(a),x)$ for every $a, b \in K$ and $x \in Q$. This means that $x = \theta_x(a)$ for every $a \in K$, $x \in Q$. □

Let C be a C-loop with nucleus $N = N(C)$. Then N is normal in C and C/N is a Steiner loop. It is not true, however, that $C/Z(C)$ is necessarily a Steiner loop. Recalling that Steiner loops are precisely inverse property loops of exponent two ([14, Lemma 2.2]), we immediately obtain:

Proposition 3.2. *Let L be a C-loop. Then $L/Z(L)$ is a Steiner loop if and only if all squares of L are central.*

Next we consider the situation where the Steiner quotient C/N is simple. Note that we do not assume that C is a C-loop in the following lemma:

Lemma 3.3. *Let C be a loop with abelian nucleus $N(C)$. If $C/N(C)$ is simple and nonassociative, then $N(C) = Z(C)$.*

Proof. Let $N = N(C)$. Consider again the homomorphism $\theta : C \to \operatorname{Aut} N; x \mapsto \theta_x = T_x|_N$. As in the proof of Theorem 2.4, $\theta_n\theta_x = \theta_x$ for every $n \in N$. Then θ induces a homomorphism $\overline{\theta} : C/N \to \operatorname{Aut} N$, $\overline{\theta}_x = \theta_x$. Assume that $\overline{\theta}$ is injective. Then $\operatorname{Im}\overline{\theta} \simeq C/N$ is nonassociative; a contradiction with $\operatorname{Im}\overline{\theta} \leq \operatorname{Aut} N$. Thus $\overline{\theta}$ is not injective. Since C/N is simple, we conclude that $\operatorname{Ker}\overline{\theta} = C/N$, i.e., $\theta_x = \mathrm{id}_N$ for every $x \in C$. Then $N(C) \leq Z(C)$ follows. □

Proposition 3.4. *Let C be a C-loop with abelian nucleus $N(C)$. If $C/N(C)$ is simple, then $N(C) = Z(C)$.*

Proof. By Lemma 3.3, we may assume $Q = C/N(C)$ is a simple, associative Steiner loop. Since Steiner loops are commutative of exponent 2, Q is either trivial or a cyclic group of order 2. In the former case, $C = N(C)$ is an abelian group and $Z(C) = N(C)$ follows. The latter case never occurs, since no nonassociative C-loop has nucleus of exponent 2, by [14, Lemma 2.9]. □

By a result of Quackenbush [15], given a Steiner triple system, either its associated Steiner quasigroup or its associated Steiner loop is simple. The hypotheses of Proposition 3.4 are therefore often fulfilled when C is a C-loop.

For the rest of the paper, we will consider only the case that the quotient $C/Z(C)$ is a Steiner loop.

The definition of a C-factor set can be greatly simplified when $\theta = \mathrm{id}$ and when Q is a Steiner loop. Except as otherwise noted, we will also write the abelian group K additively.

Proposition 3.5. *Let Q be a Steiner loop, K an abelian group and $f : Q \times Q \to K$ a map satisfying (1). Then the following conditions are equivalent:*

(i) *(id, f) is a C-factor set,*

(ii) *for every $x, y, z \in Q$, f satisfies*

$$f(y, z) + f(y, yz) = f(x, y) + f(xy, y), \tag{4}$$

(iii) *for every $x, y, z \in Q$, f satisfies the two conditions*

$$f(xy, y) = f(y, y) - f(x, y), \tag{5}$$

$$f(y, yz) = f(y, y) - f(y, z). \tag{6}$$

Proof. Since Q satisfies $y \cdot yz = z$ and $xy \cdot y = x$, (4) is equivalent to (2). Assume that (4) holds. Then (5) is obtained from (4) with $z = 1$, and (6) is obtained from (4) with $x = 1$. Conversely, assume that (5), (6) hold. Then subtracting (5) from (6) gives (4). □

The advantage of equations (5), (6) over (4) is that they deal with only 2 elements at a time, and are therefore easier to verify. By imposing another condition on f, the equations become even simpler.

Lemma 3.6. *Let Q be a Steiner loop, K an abelian group, and $f : Q \times Q \to K$ a map satisfying (1) and $f(y, y) = 0$ for every $y \in L$. Then $K \ltimes^{f}_{\mathrm{id}} Q$ is a C-loop if and only if both*

$$f(xy, y) = -f(x, y), \tag{7}$$
$$f(y, yz) = -f(y, z) \tag{8}$$

hold for every $x, y, z \in L$.

4. The building blocks of central extensions

We now build all central extensions with Steiner quotient Q. We construct all of them from small pieces arising from the underlying Steiner triple system.

In a sense, all Steiner loops are locally the same. Consider a Steiner loop Q and $x, y \in Q$ with $1 \neq x \neq y \neq 1$. Since $\{x, y\}$ is one of the edges of the underlying Steiner triple system, the subloop $\langle x, y\rangle$ generated by $\{x, y\}$ corresponds to one triangle (block) of the Steiner triple system, and is isomorphic to the Klein group.

Since the defining equations (5), (6) of a central C-factor set for Q Steiner deal only with two elements at a time, the map f can be build by small pieces:

Proposition 4.1. *Let Q be a Steiner loop, K an abelian group, and $f : Q \times Q \to K$ a map. Then (id, f) is a C-factor set if and only if for every $u, v \in Q$ with $1 \neq u \neq v \neq 1$ there are $a, b, c, d \in K$ such that $f|_{\langle u,v\rangle \times \langle u,v\rangle}$ is given by*

f	1	u	v	uv
1	0	0	0	0
u	0	a	$a+b-c-d$	$-b+c+d$
v	0	d	b	$b-d$
uv	0	$a-d$	$-a+c+d$	c

(9)

Proof. Let u, $v \in Q$ be such that $1 \neq u \neq v \neq 1$. Then $\langle u, v\rangle = \{1, u, v, w\}$, where $w = uv$. Our task is to define $f|_{\langle u,v\rangle \times \langle u,v\rangle}$ so that it satisfies (5), (6). Since we must have $f(1, x) = f(x, 1) = 0$ by (1), it remains to determine the nine entries $f(u, u)$, $f(u, v)$, $\ldots$, $f(v, w)$, $f(w, w)$. We think of the entries as variables.

Condition (5) yields 6 equations in these variables, but only three of these equations are distinct, namely

$$f(u, v) = f(v, v) - f(w, v),$$
$$f(u, w) = f(w, w) - f(v, w),$$
$$f(v, u) = f(u, u) - f(w, u).$$

Similarly, condition (6) yields additional three equations

$$f(u, v) = f(u, u) - f(u, w),$$
$$f(v, u) = f(v, v) - f(v, w),$$
$$f(w, u) = f(w, w) - f(w, v).$$

When we reorder the variables as $f(u,u)$, $f(v,v)$, $f(w,w)$, $f(u,v)$, $f(u,w)$, $f(v,u)$, $f(v,w)$, $f(w,u)$, $f(w,v)$, the above equations correspond to the system of linear equations $A\overrightarrow{x} = \overrightarrow{0}$, where

$$A = \begin{pmatrix} 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & -1 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & -1 & 0 & -1 & 0 \\ 1 & 0 & 0 & -1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & -1 \end{pmatrix}.$$

By keeping the 3rd, 5th and 6th row of A, it is now easy to see that by subtracting rows from each other and by multiplying rows by -1, the system A is equivalent to

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & -1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & 1 & 0 & -1 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & -1 & -1 \end{pmatrix}.$$

Therefore the variables $f(u,u) = a$, $f(v,v) = b$, $f(w,w) = c$, and $f(v,u) = d$ can be chosen arbitrarily, and the remaining variables are as claimed in (9). □

Let us call a 4×4 array with entries from an abelian group K a *block* (*over* K) if it is of the form (9) for some $a, b, c, d \in K$.

An arbitrary C-factor set (id, f) with Q Steiner can then be obtained as follows: (i) assign $f(1,x) = f(x,1) = 0$ for every $x \in Q$, (ii) assign the diagonal entries $f(x,x)$ with $x \neq 1$ arbitrarily, (iii) if f is not completed, assign arbitrarily any available $f(x,y)$, complete the corresponding block $f|_{\langle x,y\rangle \times \langle x,y\rangle}$ and repeat step (iii).

Note that this implies that for every block B and for every Steiner loop Q there is a C-factor set (id, f) such that $f|_{\langle u,v\rangle \times \langle u,v\rangle} = B$ for some u, $v \in Q$.

If one block B is fixed, and when for every u, $v \in Q$ with $1 \neq u \neq v \neq 1$ it is possible to premute u, v, uv so that $f|_{\langle u,v\rangle \times \langle u,v\rangle} = B$, we say that the C-factor set (id, f) is *based on the block* B.

After a short reflection we see that:

Lemma 4.2. *Let B be a block with diagonal entries $a, b, c \in K$ such that $a = b = c$. Then there is a C-factor set (id, f) based on B.*

For instance, the two blocks

$$B_1(a) = \begin{array}{c|cccc} f & 1 & u & v & uv \\ \hline 1 & 0 & 0 & 0 & 0 \\ u & 0 & a & a & 0 \\ v & 0 & 0 & a & a \\ uv & 0 & a & 0 & a \end{array}, \qquad B_2(d) = \begin{array}{c|cccc} f & 1 & u & v & uv \\ \hline 1 & 0 & 0 & 0 & 0 \\ u & 0 & 0 & -d & d \\ v & 0 & d & 0 & -d \\ uv & 0 & -d & d & 0 \end{array}$$

give rise to C-factor sets (not necessarily uniquely determined). We will take advantage of these blocks in the next section.

When the diagonal entries a, b, c of B are not all the same, no C-factor set (id, f) is based on B provided Q is sufficiently large:

Lemma 4.3. *Let B be a block with diagonal entries a, b, c such that $|\{a, b, c\}| \geq 2$. If $|Q| > 4$ then no C-factor set (id, f) is based on B.*

Proof. Assume that f is based on B. Let u, $v \in Q$, $1 \neq u \neq v \neq 1$. Then $f|_{\langle u,v\rangle\times\langle u,v\rangle} = B$, and we can assume without loss of generality that $f(u,u) = a$, $f(v,v) = b$. Furthermore, we can assume that c occurs once among a, b, c. Since $|Q| > 4$, there are x, $y \in Q \setminus \langle u,v\rangle$ such that $xy = u$. Since f is based on B, we have $f(x,x) = b$, $f(y,y) = c$, say. Now, $f|_{\langle v,x\rangle\times\langle v,x\rangle}$ contains c at least twice among its diagonal entries, showing that f is not based on B after all. □

Example 4.4. Let us illustrate the Lemma with the block

$$B_3(a) = \begin{array}{c|cccc} f & 1 & u & v & uv \\ \hline 1 & 0 & 0 & 0 & 0 \\ u & 0 & 0 & 0 & 0 \\ v & 0 & -a & 0 & a \\ uv & 0 & a & 0 & a \end{array}$$

and with the smallest nonassociative Steiner loop of order 10:

Q	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	0	3	2	5	4	7	6	9	8
2	2	3	0	1	6	9	4	8	7	5
3	3	2	1	0	8	7	9	5	4	6
4	4	5	6	8	0	1	2	9	3	7
5	5	4	9	7	1	0	8	3	6	2
6	6	7	4	9	2	8	0	1	5	3
7	7	6	8	5	9	3	1	0	2	4
8	8	9	7	4	3	6	5	2	0	1
9	9	8	5	6	7	2	3	4	1	0

(We used the block $B_3(a)$ in [14, Proposition 3.4], without calling it "block", to construct the smallest nonassociative noncommutative C-loop. Furthermore, the multiplication table of the 10-element Steiner loop is obtained from that of [14] by interchanging the elements 6 and 9. The current multiplication table is more suitable here, as we will see.)

Consider the subloop $\{0,1,2,3\}$. Define $f|_{\langle 1,2\rangle\times\langle 1,2\rangle}$ so that it coincides with $B_3(a)$. It is possible to extend f so that $f|_{\langle 1,k\rangle\times\langle 1,k\rangle}$ coincides with $B_3(a)$ for every $k > 0$. The partial map f then looks as follows:

Q	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	a	0	a	0	a	0	a	0	a
2	0	a	0	$-a$						
3	0	0	0	0						
4	0	a			0	$-a$				
5	0	0			0	0				
6	0	a					0	$-a$		
7	0	0					0	0		
8	0	a							0	$-a$
9	0	0							0	0

However, $f|_{\langle 2,4\rangle\times\langle 2,4\rangle}$ then shows that f is not based on $B_3(a)$, no matter how it is actually defined.

5. Nonflexible C-loops with prescribed center and factor by center

In this section, we determine for which abelian groups K and Steiner loops Q there exist nonflexible (hence noncommutative) C-loops C with center K and factor $C/K = Q$. Much of the discussion applies to nuclear extensions as well.

Let us first say more about flexibility in extensions of C-loops:

Lemma 5.1. *In a C-loop C with central squares, the following conditions are equivalent.*

(i) *C is flexible.*
(ii) *$(xy)^2 = (yx)^2$ for all $x, y \in C$.*
(iii) *$x \mapsto x^3$ is an antiautomorphism.*

Proof. First, $x(xy)^2 = x^2y \cdot xy = x^2(y \cdot xy)$ and so $(xy)^2 = x(y \cdot xy)$. Next, $x(yx)^2 = (yx)^2x = yx \cdot yx^2 = (yx \cdot y)x^2 = x^2(yx \cdot y)$ and so $(yx)^2 = x(yx \cdot y)$. This shows the equivalence of (i) and (ii).

Next, $(xy)^2 = (xy)^3 \cdot y^{-1}x^{-1}$ and $(yx)^2 = yx \cdot (y^2y^{-1} \cdot x^2x^{-1}) = y^3x^3 \cdot y^{-1}x^{-1}$. This shows the equivalence of (ii) and (iii). □

Corollary 5.2. *A C-loop of exponent 4 with central squares is flexible.*

Proof. As noted, C-loops are inverse property loops. In any inverse property loop of exponent n, $x \mapsto x^{n-1} = x^{-1}$ is an antiautomorphism, and so the result follows from Lemma 5.1. □

Corollary 5.3. *A C-loop with nucleus of order 2 is flexible.*

Proof. By [14, Proposition 2.4], the nucleus of a C-loop contains every square. In any loop with nucleus of order 2, the nucleus coincides with the center. Now apply Corollary 5.2. □

Corollary 5.4. *Let Q be a Steiner loop, K an abelian group, and (id, f) a C-factor set. Then $K \ltimes^f_{\mathrm{id}} Q$ is flexible if and only if $2f(x, y) = 2f(y, x)$ for all $x, y \in Q$.*

Proof. For $a, b \in K$, $x, y \in Q$, we compute

$$((a, x) * (b, y))^2 = (2a + 2b + 2f(x, y) + f(xy, xy),\ 1).$$

Reversing the roles of (a, x) and (b, y), we see that condition (ii) of Lemma 5.1 is satisfied if and only if $2f(x, y) = 2f(y, x)$ for all $x, y \in Q$. □

We are now ready to characterize the parameters $K = Z(C)$, $Q = C/K$ of nonflexible C-loops.

Lemma 5.5. *Let C be a nonflexible C-loop with center K, and let $Q = C/K$. Then $|Q| > 2$ and K is not an elementary abelian 2-group.*

Proof. If $|Q| = 1$, then C is associative, hence flexible. If $|Q| = 2$, then C has nucleus of index 2, which is impossible by [14, Lemma 2.9].

Note that $C = K \ltimes^f_{\mathrm{id}} Q$ for some C-factor set (id, f) by Lemma 3.1. If K is an elementary abelian 2-group, then $2f(x, y) = 0$ for every $x, y \in Q$. Then C is flexible by Corollary 5.4. □

Lemma 5.6. *Let Q be a Steiner loop with $|Q| > 2$, and let K be an abelian group which is not an elementary abelian 2-group. Then there exists a nonflexible C-loop C of order $|Q| \cdot |K|$ such that the nucleus $N = N(C)$ is isomorphic to K, and such that C/N is isomorphic to Q. Moreover, $N = Z(C)$.*

Proof. Let $a \in K$ be an element of order different from 1 or 2. By Lemma 4.2, there is a C-factor set (id, f) with $f : Q \times Q \to K$ based on the block $B = B_1(a)$. Let $C = K \ltimes^f_{\mathrm{id}} Q$ be the corresponding C-loop. Given $1 \neq x \in Q$, we see from B that there is $y \in Q$ such that $f(x, y) = a$ and $f(y, x) = 0$. Corollary 5.4 then shows that C is not flexible. In fact, a quick calculation yields $(b, x)(c, y) \cdot (b, x) \neq (b, x) \cdot (c, y)(b, x)$, where we choose y as above, and where $b, c \in K$ are arbitrary. Since $N \leq K$ by Theorem 2.4, $N = K$ follows. By Lemma 3.1, $N = Z(C)$. □

In summary:

Theorem 5.7. *A nonflexible C-loop C with center K and Steiner factor $C/K = Q$ exists if and only if Q is a Steiner loop with $|Q| > 2$ and K is not an elementary abelian 2-group. Moreover, it is possible to demand $Z(C) = N(C)$ in such a case.*

5.1. **Nonflexible C-loops with prescribed abelian nucleus and factor by nucleus.** We now turn to the following related question:

Problem 5.8. *For which abelian groups K and Steiner loops Q does there exist a nonflexible C-loop C with nucleus K and $C/K = Q$?*

Theorem 5.7 gives a partial answer. Corollary 5.3 implies that $|K| > 2$. Lemma 2.9 of [14] implies that $|Q| > 2$. Thus the only situation that remains to be considered is: K an elementary abelian 2-group of order greater than 2, and Q a Steiner loop of order greater than 2.

Lemma 5.9. *Let Q be the Klein group and K an elementary abelian 2-group with $|K| > 2$. Then there exists a nonflexible C-loop C such that $N(C) = K$ and $C/K = Q$.*

Proof. Let $Q = \{1, u, v, w\}$. Assume first that $K = Q$. (We thus return to the multiplicative notation for K in this proof.) Define $\theta : Q \to \mathrm{Aut}\, K$ by $\theta_1 = \theta_u = \mathrm{id}_K$, $\theta_v = \theta_w = (v, w)$, where (v, w) is the transposition of v and w. Define $f : Q \times Q \to K$ by

f	1	u	v	w
1	1	1	1	1
u	1	1	1	1
v	1	v	1	w
w	1	v	1	v

.

A straightforward but tedious verification of condition (2) then shows that (θ, f) is a C-factor set. Moreover,

$$\begin{aligned}(u, v)(v, u) &= (u\theta_v v f(v, u), vu) = (uwv, w) = (1, w)\\ &\neq (w, w) = (vu, w) = (v\theta_u u f(u, v), uv) = (v, u)(u, v).\end{aligned}$$

and consequently

$$\begin{aligned}(u, v)(v, u) \cdot (u, v) &= (1, w)(u, v) = (\theta_w u f(w, u), wv) = (uv, u) = (w, u)\\ &\neq (1, u) = (uvw, u) = (u\theta_v w f(v, w), vw) = (u, v)(w, w) = (u, v) \cdot (v, u)(u, v).\end{aligned}$$

Thus $C_{16} = K \ltimes^f_\theta Q$ is a nonflexible C-loop with the desired nucleus and nuclear factor.

To obtain a C-loop whose nucleus is a given elementary abelian 2-group K, $|K| = 2^m > 4$ and with nuclear factor Q, it suffices to take the direct product of the loop C_{16} with the elementary abelian 2-group of order 2^{m-2}. □

TABLE 1. A smallest nonflexible noncommutative C-loop with nucleus that is an elementary abelian 2-group

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

Table 1 gives a multiplication table of one of smallest nonflexible noncommutative C-loops with nucleus isomorphic to the Klein group. The loop is constructed via the extension described in the proof of Lemma 5.9.

We have not been able to fully answer Problem 5.8. Note, however, that it is not possible to prescribe an arbitrary quotient Q, since Lemma 3.3 and Theorem 5.7 imply:

Corollary 5.10. *Let K be an elementary abelian 2-group and Q a simple Steiner loop. Then there is no nonflexible C-loop C with nucleus K and $C/K = Q$.*

5.2. **Associators of given orders.** Consider [14, Proposition 3.4] restated in terms of blocks:

Proposition 5.11. *Let $Q = \{1, u, v, uv\}$ be the Klein group. Let K be an abelian group and $a \in K$ an element of order at least 3. Assume that $f : Q \times Q \to K$ is based on the block $B_3(a)$. Then $K \ltimes^f_{\mathrm{id}} Q$ is a nonflexible C-loop with nucleus and center $Z = N = \{(a, 1);\ a \in K\}$.*

The extension of Proposition 5.11 allows us to construct a nonflexible C-loop with an associator of given order $n > 2$.

Let $n > 2$, $\langle a \rangle = K = (\mathbb{Z}_n, +)$, $Q = \{1, u, v, w\}$ and f be as in Proposition 5.11. Let $x = (0, w)$, $y = (0, u)$, $z = (a, w) \in C = K \ltimes^f_{\mathrm{id}} Q$. Then $((xy)z)^{-1} = ((0, w)(0, u) \cdot (a, w))^{-1} = ((a, v)(a, w))^{-1} = (3a, u)^{-1} = (-3a, u)$. Also, $x \cdot yz = (0, w) \cdot (0, u)(a, w) = (0, w)(a, v) = (a, u)$. Therefore the associator of x, y, z is equal to $[x, y, z] = (xy \cdot z)^{-1} \cdot (x \cdot yz) = (-3a, u)(a, u) = (-2a, 1)$. It follows that the order of $[x, y, z]$ is n when n is odd, and $n/2$ when n is even.

Corollary 5.12. *For every $n > 2$ there is a nonflexible C-loop C containing an associator of order n. Moreover, it is possible to have $|C| = 4n$ if n is odd, and $|C| = 8n$ if n is even.*

Corollary 5.12 should be contrasted with the case of extra loops. In an extra loop, every associator has order 2 [9, Theorem 5.7].

We have some evidence for the following:

Conjecture 5.13. *Let C be a C-loop with an associator of order n. Then $|C| \geq 4n$ if n is odd, and $|C| \geq 8n$ if n is even.*

6. The standard Cayley-Dickson process

In view of Proposition 5.11 and Corollary 5.3, it is now natural to ask if there is a flexible, nonextra, noncommutative C-loop with nucleus (hence center) of order 2. The answer is "yes", as we will see in §7, and the loop can be obtained in a classical way—by the standard Cayley-Dickson process, which we deliberately define in a broad way here.

The notation and terminology of this section are taken mostly from [18].

By an *algebra* we mean here a vector space (over a field F) with multiplication that distributes over addition, and with a neutral element 1 with respect to multiplication. In particular, we do not assume that the multiplication is associative.

6.1. **The process.** Let D be a finite-dimensional algebra over F, let $N_D : D \to F$ be a quadratic form, and set $\lambda = -1 \in F$. Let $\langle\ ,\ \rangle_D : D \oplus D \to F$ be the associated bilinear form defined by $\langle x, y\rangle_D = N_D(x+y) - N_D(x) - N_D(y)$, and let $\overline{x} = \langle x, 1\rangle_D 1 - x$ be the *conjugate* of $x \in D$.

We say that (C, N_C) is obtained from (D, N_D) by *standard doubling* if

(i) $C = D \oplus D$ as a vector space,

(ii) the multiplication in C is given by

$$(x, y)(u, v) = (xu + \lambda\overline{v}y, vx + y\overline{u}), \tag{10}$$

(iii) $N_C((x, y)) = N_D(x) - \lambda N_D(y)$.

Since $\langle\ ,\ \rangle_D$ is bilinear, it follows that conjugation is an additive homomorphism, and it is easy to check that C is an algebra and that N_C is a quadratic form. It is therefore possible to iterate the standard doubling. It is customary to call these iterations the *standard Cayley-Dickson process.*

6.2. **Structure constants.** The presence of the distributive laws makes it possible and convenient to describe the multiplication in D by *structure constants.* In particular, when $\{d_1, \ldots, d_n\}$ is a basis for D, then there are n^3 constants $\gamma_{ij}^k \in F$ such that $d_i d_j = \sum_{k=1}^n \gamma_{ij}^k d_k$.

By selecting the basis of D carefully and systematically in the standard doubling, all but one structure constants can be eliminated for given i, j, as we are going to show. (The usual multiplication formulae for quaternions and octonions are based on this observation.)

Lemma 6.1. *Assume that (C, N_C) is obtained from (D, N_D) by one application of doubling. Then $\overline{(u, v)} = (\overline{u}, -v)$ for every u, $v \in D$.*

Proof. We have $\overline{(u, v)} = \langle (u, v), (1, 0)\rangle_C (1, 0) - (u, v) = [N_C((u, v) + (1, 0)) - N_C(u, v) - N_C(1, 0)](1, 0) - (u, v) = [N_D(u+1) + N_D(v) - N_D(u) - N_D(v) - N_D(1) - N_D(0)](1, 0) - (u, v) = \langle u, 1\rangle_D (1, 0) - (u, v) = (\overline{u} + u)(1, 0) - (u, v) = (\overline{u}, -v)$. □

Lemma 6.2. *Let D be an algebra over F, $N_D : D \to F$ a quadratic form, and let (C, N_C) be obtained from (D, N_D) by the standard doubling. Suppose that $\{d_1, \ldots, d_n\}$ is a basis of D such that:*

(i) $d_1 = 1$,
(ii) $\overline{d_i} = -d_i$ *for* $1 < i \leq n$,
(iii) $d_i d_j \in \pm\{d_1, \ldots, d_n\}$ *for* $1 \leq i,\ j \leq n$,
(iv) $d_i d_i = -1$ *for* $1 < i \leq n$,
(v) $d_i d_j = -d_j d_i$ *for* $1 < i < j \leq n$,
(vi) $\overline{d_i d_j} = \overline{d_j} \cdot \overline{d_i}$, $\overline{\overline{d_i}} = d_i$, *for* $1 \leq i,\ j \leq n$,
(vii) $d_i(d_i d_j) = (d_i d_i)d_j$, $d_i(d_j d_j) = (d_i d_j)d_j$, $(d_i d_j)d_i = d_i(d_j d_i)$ *for* $1 \leq i,\ j \leq n$.

For $1 \leq i \leq n$, *let* $c_i = (d_i, 0)$, $c_{i+n} = (0, d_i)$. *Then* $\{c_1, \ldots, c_{2n}\}$ *is a basis of* C *satisfying the properties analogous to* (i)–(vii), *with* $2n$ *instead of* n.

Proof. This follows from straightforward calculation, but we show most of the proof for completeness.

Part (i) is trivial. By Lemma 6.1, $\overline{(d_i, 0)} = (\overline{d_i}, 0) = (-di, 0)$, $\overline{(0, d_i)} = (0, -d_i)$ for every $1 < i \leq n$, and (ii) follows.

While multiplying c_i by c_j, we notice that only one of the four summands in (10) is nonzero, and this nonzero summand has coefficient ± 1. Namely, for $1 \leq i,\ j \leq n$, we have

$$c_i c_j = (d_i d_j, 0), \quad c_i c_{j+n} = (0, d_j d_i), \quad c_{i+n} c_j = (0, d_i \overline{d_j}), \quad c_{i+n} c_{j+n} = (-\overline{d_j} d_i, 0).$$

This shows (iii).

Part (iv) is easy, and we proceed to prove (v). With $1 < i < j \leq n$ we get $c_i c_j = (d_i d_j, 0) = (-d_j d_i, 0) = -c_j c_i$. With $1 < i \leq n$, $1 \leq j \leq n$ we get $c_i c_{j+n} = (0, d_j d_i) = -(0, d_j \overline{d_i}) = -c_{j+n} c_i$. When $1 \leq i < j \leq n$, we have $c_{i+n} c_{j+n} = (-\overline{d_j} d_i, 0) = -(-\overline{d_i} d_j, 0) = -c_{j+n} c_{i+n}$.

Part (vi) is similar, and can be simplified by noting that it suffices to prove (vi) for $i < j$.

We now prove $c_i(c_i c_j) = (c_i c_i)c_j$ for $1 \leq i,\ j \leq 2n$, and leave the other two parts of (vii) to the reader. There is nothing to show when $i = 1$ or $j = 1$. When $i > 1$, the equation becomes $c_i(c_i c_j) = -c_j$. With $1 < i,\ j \leq n$, we then get $c_i(c_i c_j) = (d_i(d_i d_j), 0) = (-d_j, 0) = -c_j$, $c_i(c_i c_{j+n}) = (d_i, 0)(0, d_j d_i) = (0, (d_j d_i)d_i) = (0, -d_j) = -c_{j+n}$, $c_{i+n}(c_{i+n} c_{j+n}) = (0, d_i)(-\overline{d_j} d_i, 0) = (0, d_i(\overline{-\overline{d_j} d_i})) = -(0, d_i(\overline{d_i} d_j)) = -(0, d_j) = -c_{j+n}$, where in the last case we allow $i = 1$. □

6.3. **Remarks on the Cayley-Dickson process.** The word *standard* in standard Cayley-Dickson process refers to the fact that $\lambda = -1$. The process makes sense for any value of $\lambda \in F^*$.

It is usually assumed that N_D is a nondegenerate quadratic form satisfying $N_D(uv) = N_D(u)N_D(v)$. Then (D, N_D) is called a *composition algebra*.

When the underlying field F is the real numbers $\mathbb{R}$, we speak of *real algebras*. Nevertheless, the characteristic of F can be arbitrary.

The classical Hurwitz theorem has been extended to all characteristics and composition algebras, i.e., composition algebras exist only in dimension 1, 2, 4 and 8. See [18, Chapter 1] for details and [18, Theorem 1.6.2] in particular.

Smith [17] constructed a real 16-dimensional composition semialgebra, which does not satisfy one of the distributive laws but otherwise has all the properties of a composition algebra. Kivunge and Smith [10] study subloops (which are not C-loops unless associative) of the associated left loop.

7. C-loops arising from the standard Cayley-Dickson process

Let A_n be the algebra of dimension 2^n constructed from $A_0 = \mathbb{R}$ with $N_{\mathbb{R}} : x \mapsto x^2$ by the standard Cayley-Dickson process. Assume that the basis $\{a_1, \dots, a_{2^n}\}$ of A_n is obtained systematically as in Lemma 6.2. Then $L_n = \pm\{a_1, \dots, a_{2^n}\}$ is closed under multiplication by Lemma 6.2(iii), and it possesses a neutral element $1 = a_1$. Note that $-a_1$ commutes and associates with all elements of L_n. Also note that the inverse of a_i is either a_i or $-a_i$, and that L_n satisfies the alternative and flexible laws, by Lemma 6.2(vii). Hence L_n is a flexible, alternative, inverse property loop.

Proposition 7.1. *For every $n \geq 1$, L_n is a flexible C-loop.*

Proof. Let x, y, $z \in L_n$. Then $x(y(yz)) = x(y^2z)$ by alternativity. By Lemma 6.2, $yy = \pm 1$, and, as we have observed, $\pm 1 \in Z(L_n)$. Therefore $x(y^2z) = (xz)y^2$. Similarly, $((xy)y)z = (xz)y^2$. □

Proposition 7.2. *For $n \geq 1$, let L_n be the C-loop of signed basic elements of A_n. Then:*

(i) $N(L_2) = Z(L_2) = L_2$,
(ii) $N(L_3) = L_3$, $Z(L_3) = \{\pm 1\}$,
(iii) $N(L_n) = Z(L_n) = \{\pm 1\}$ *for every* $n > 0$, $n \notin \{2, 3\}$.

Proof. Using the standard notation for complex numbers and quaternions, we have $L_1 = \{\pm 1\}$, $L_2 = \{\pm 1, \pm i\} \cong \mathbb{Z}_4$, $L_3 = \{\pm 1, \pm i, \pm j, \pm k\} \cong Q$, where Q is the quaternion group. It remains to show (iii).

We will demonstrate later (outside of this proof) that (iii) holds for L_4. Assume that (iii) holds for every L_m with $4 \leq m \leq n$.

If $x = (u, 0)$ for $u \in L_n \setminus \{\pm 1\}$ then $x \notin N(L_n)$ by induction assumption, and since $L_n \leq L_{n+1}$, we have $x \notin N(L_{n+1})$.

Assume that $x = (0, u)$ for $u \in L_n$. For $v, w \in L_n$, we have

$$(0, 1)(v, 0) \cdot (0, w) = (0, \overline{v})(0, w) = (-\overline{w} \cdot \overline{v}, 0), \tag{11}$$

$$(0, 1) \cdot (v, 0)(0, w) = (0, 1)(0, wv) = (-\overline{wv}, 0). \tag{12}$$

When $u = \pm 1$, pick $v, w \in L_n$ that do not commute (which is possible by Lemma 6.2), and conclude from (11)), (12)) that $(0, u) \notin N(L_{n+1})$. When $u \neq \pm 1$, let $u = w$, pick $v \in L_n$ that does not commute with u, and conclude as in the previous case that $(0, u) \notin N(L_{n+1})$. □

7.1. **The standard sedenion loop.** The C-loop $S = L_4 = \pm\{a_1, \dots, a_{16}\}$ is called the *standard sedenion loop*. The "structure constants" $a_i a_j = \gamma_{ij}$ of the 16-dimensional algebra A_4 are as in Table 2, where i stands for a_i, and $-i$ for $-a_i$.

The loop S is then easily obtained. By Proposition 7.1, S is a flexible C-loop. One can check by hand (or by computer) that $N(S) = Z(S) = \{\pm 1\}$, thus completing the proof of Proposition 7.2.

Moreover, S is not extra. Therefore any of the loops L_n, $n > 3$, is a flexible, nonextra, noncommutative C-loop with nucleus of order 2. These are the loops we set out to find at the beginning of §6.

More detailed information about the standard sedenion loop, including its subloop structure, can be found in [3]. The loop S is contained in the library of loops of the GAP [7] package LOOPS [12]. The above-mentioned properties of S can be verified easily with LOOPS.

TABLE 2. Structure constants of the standard real sedenions S

γ_{ij}	1	2	3	4	5	6	7	8	9	19	11	12	13	14	15	16
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	2	−1	4	−3	6	−5	−8	7	10	−9	−12	11	−14	13	16	−15
3	3	−4	−1	2	7	8	−5	−6	11	12	−9	−10	−15	−16	13	14
4	4	3	−2	−1	8	−7	6	−5	12	−11	10	−9	−16	15	−14	13
5	5	−6	−7	−8	−1	2	3	4	13	14	15	16	−9	−10	−11	−12
6	6	5	−8	7	−2	−1	−4	3	14	−13	16	−15	10	−9	12	−11
7	7	8	5	−6	−3	4	−1	−2	15	−16	−13	14	11	−12	−9	10
8	8	−7	6	5	−4	−3	2	−1	16	15	−14	−13	12	11	−10	−9
9	9	−10	−11	−12	−13	−14	−15	−16	−1	2	3	4	5	6	7	8
10	10	9	−12	11	−14	13	16	−15	−2	−1	−4	3	−6	5	8	−7
11	11	12	9	−10	−15	−16	13	14	−3	4	−1	−2	−7	−8	5	6
12	12	−11	10	9	−16	15	−14	13	−4	−3	2	−1	−8	7	−6	5
13	13	14	15	16	9	−10	−11	−12	−5	6	7	8	−1	−2	−3	−4
14	14	−13	16	−15	10	9	12	−11	−6	−5	8	−7	2	−1	4	−3
15	15	−16	−13	14	11	−12	9	10	−7	−8	−5	6	3	−4	−1	2
16	16	15	−14	−13	12	11	−10	9	−8	7	−6	−5	4	3	−2	−1

REFERENCES

[1] V. D. Belousov, *Foundations of the Theory of Quasigroups and Loops* (Russian), *Izdat. "Nauka"*, Moscow, 1967. MR 36#1569, Zbl 0163.01801.

[2] R. H. Bruck, *A Survey of Binary Systems*, 3rd printing, corrected, *Ergebnisse der Mathematik und ihrer Grenzgebiete*, *Neue Folge* **20**, Springer-Verlag, 1971. MR 20#76, Zbl 0206.30301.

[3] R. Cawagas, On the structure and zero divisors of the Cayley-Dickson sedenion algebra, *Discuss. Math. Gen. Algebra Appl.*, to appear.

[4] O. Chein, H. O. Pflugfelder, and J. D. H. Smith, eds., *Quasigroups and Loops: Theory and Applications*, Heldermann Verlag, 1990. MR 93g:20133, Zbl 0719.20036.

[5] F. Fenyves, Extra loops I, *Publ. Math. Debrecen* **15** (1968) 235–238. MR 38#5976, Zbl 0172.02401.

[6] F. Fenyves, Extra loops II: On loops with identities of Bol-Moufang type, *Publ. Math. Debrecen* **16** (1969), 187–192. MR 41#7017, Zbl 0221.20097.

[7] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4*; 2004, `http://www.gap-system.org`.

[8] M. K. Kinyon and K. Kunen, The structure of extra loops, *Quasigroups and Related Systems*, to appear.

[9] M. K. Kinyon, K. Kunen, and J. D. Phillips, Diassociativity in conjugacy closed loops, *Comm. Algebra* **32** (2004) 767–786.

[10] B. Kivunge and J. D. H. Smith, Subloops of sedenions, *Comment. Math. Univ. Carolinae* **45** (2004) 295–302.

[11] F. Leong, The devil and angel of loops, *Proc. Amer. Math. Soc.* **54** (1976), 32–34. MR 52#10940, Zbl 0361.20067.

[12] Gábor P. Nagy and Petr Vojtěchovský, *LOOPS: a package for GAP* 4, beta version available at `http://www.math.du.edu/loops`

[13] H. O. Pflugfelder, *Quasigroups and Loops: Introduction*, *Sigma Series in Pure Mathematics* **7**, Heldermann Verlag, 1990. MR 93g:20132, Zbl 0719.20036.

[14] J. D. Phillips and P. Vojtěchovský, C-loops: An Introduction, *Publ. Math. Debrecen.*, to appear.

[15] R. W. Quackenbush, Varieties of Steiner loops and Steiner quasigroups, *Canad. J. Math.* **28** (1976), 1187–1198. MR 54#12946, Zbl 0359.20070.

[16] J. J. Rotman, *An Introduction to the Theory of Groups*, 4th edition, *Graduate Texts in Mathematics* **148**, Springer-Verlag, 1995. MR 95m:20001, Zbl 0810.20001.

[17] J. D. H. Smith, A left loop on the 15-sphere, *J. Algebra* **176** (1995), 128–138. MR 96j:20088, Zbl 0841.17004.

[18] T. A. Springer and F. D. Veldkamp, *Octonions, Jordan Algebras and Exceptional Groups*, *Springer Monographs in Mathematics*, Springer Verlag, 2000. MR 2001f:17006, Zbl pre01465056.

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 & Computer Science, Wabash College, Crawfordsville, IN 47933 U.S.A.
E-mail address: phillipj@wabash.edu
URL: http://www.wabash.edu/depart/math/faculty.html#Phillips

Department of Mathematics, University of Denver, 2360 S Gaylord St, Denver, CO 80208 U.S.A.
E-mail address: petr@math.du.edu
URL: http://www.math.du.edu/~petr