Automorphism groups of real Cayley-Dickson loops

Jenya Kirshtein *

Abstract

The Cayley-Dickson loop $\mathcal{C}_n$ is the multiplicative closure of basic elements of the algebra constructed by n applications of the Cayley-Dickson doubling process (the first few examples of such algebras are real numbers, complex numbers, quaternions, octonions, sedenions). We will discuss properties of the Cayley-Dickson loops, show that these loops are Hamiltonian and describe the structure of their automorphism groups.

1 The Cayley-Dickson doubling process

The Cayley-Dickson doubling produces a sequence of power-associative algebras over a field. The dimension of the algebra doubles at each step of the construction. We consider the construction on $\mathbb{R}$, the field of real numbers.

Let $\mathbb{A}_0 = \mathbb{R}$ with conjugation $a^* = a$ for all $a \in \mathbb{R}$. Let $\mathbb{A}_{n+1} = \{(a,b) \mid a,b \in A_n\}$ for $n \in \mathbb{N}$, where multiplication, addition and conjugation are defined as follows:

$$(a,b)(c,d) = (ac - d^*b, da + bc^*), \tag{1}$$
$$(a,b) + (c,d) = (a+c, b+d), \tag{2}$$
$$(a,b)^* = (a^*, -b). \tag{3}$$

Conjugation defines a norm $\|a\| = (aa^*)^{1/2}$ and the multiplicative inverse for nonzero elements $a^{-1} = a^*/\|a\|^2$. Notice that $(a,b)(a,b)^* = (\|a\|^2 + \|b\|^2, 0)$ and $(a^*)^* = a$. Dimension of $\mathbb{A}_n$ over $\mathbb{R}$ is 2^n.

Definition 1. *A nontrivial algebra A over a field is a division algebra if for any nonzero $a \in A$ and any $b \in A$ there is a unique $x \in A$ such that $ax = b$ and a unique $y \in A$ such that $ya = b$.*

Definition 2. *A normed division algebra A is a division algebra over the real or complex numbers which is a normed vector space, with norm $\|\cdot\|$ satisfying $\|xy\| = \|x\|\,\|y\|$ for all $x, y \in A$.*

Theorem 3. ***(Hurwitz, 1898 [5])*** *The only normed division algebras over $\mathbb{R}$ are $\mathbb{A}_0 = \mathbb{R}$ (real numbers), $\mathbb{A}_1 = \mathbb{C}$ (complex numbers), $\mathbb{A}_2 = \mathbb{H}$ (quaternions) and $\mathbb{A}_3 = \mathbb{O}$ (octonions).*

2 Cayley-Dickson loops and their properties

We will consider multiplicative structures that arise from the Cayley-Dickson doubling process.

Definition 4. *A loop is a nonempty set L with binary operation $\cdot$ such that*

*Department of Mathematics, University of Denver, Denver, CO 80208, USA

1. *there is a neutral element* $id \in L$ *such that* $id \cdot x = x \cdot id = x$ *for all* $x \in L$,

2. *for all* $x, z \in L$ *there is a unique* y *such that* $x \cdot y = z$,

3. *for all* $y, z \in L$ *there is a unique* x *such that* $x \cdot y = z$.

Define Cayley-Dickson loops $(\mathcal{C}_n, \cdot)$ inductively as follows:

$$\begin{aligned} \mathcal{C}_0 &= \{\pm(1)\}, \mathcal{C}_1 = \{\pm(1,0), \pm(1,1)\}, \\ \mathcal{C}_n &= \{\pm(x_1, x_2, \ldots, x_n, 0), \pm(x_1, x_2, \ldots, x_n, 1) \mid (x_1, x_2, \ldots, x_n) \in \mathcal{C}_{n-1}\}, n \in \mathbb{N}. \end{aligned}$$

In a compact form,

$$\mathcal{C}_0 = \{\pm(1)\}, \quad \mathcal{C}_n = \{\pm(x,0), \pm(x,1) \mid x \in \mathcal{C}_{n-1}\}, \quad n \in \mathbb{N}. \tag{4}$$

Using this approach, multiplication (1) becomes

$$(x,0)(y,0) = (xy, 0), \tag{5}$$
$$(x,0)(y,1) = (yx, 1), \tag{6}$$

$$(x,1)(y,0) = (xy^*, 1), \tag{7}$$
$$(x,1)(y,1) = (-y^* x, 0). \tag{8}$$

Conjugation (3) modifies to

$$(x,0)^* = (x^*, 0), \tag{9}$$
$$(x,1)^* = (-x, 1). \tag{10}$$

All elements of $\mathcal{C}_n$ have norm one due to the fact that

$$\|(x, x_{n+1})\| = \|x\| = \|(x_1, \ldots, x_n)\| = \ldots = \|x_1\| = 1, \tag{11}$$

however, not all the elements of $\mathbb{A}_n$ of norm one are in $\mathcal{C}_n$. We will write $\mathcal{C}_n$ instead of $(\mathcal{C}_n, \cdot)$ further in the text. The Cayley-Dickson loop is the multiplicative closure of basic elements of the corresponding Cayley-Dickson algebra. Denote a basic element i_k of $\mathcal{C}_n$ to be the element in which, reading from right to left, the n-digit binary representation of k, $k \in \{0, .., 2^n - 1\}$, is followed by 1; replace i_0 with 1. The first few examples of the Cayley-Dickson loops are the real group $\mathbb{R}_2$ (abelian); the complex group $\mathbb{C}_4$ (abelian); the quaternion group $\mathbb{H}_8$ (not abelian); the octonion loop $\mathbb{O}_{16}$ (Moufang); the sedenion loop $\mathbb{S}_{32}$ (not Moufang); the loop $\mathbb{T}_{64}$. For example,

$$\begin{aligned} \mathcal{C}_2 = \mathbb{H}_8 &= \{(1,0,0), -(1,0,0), (1,1,0), -(1,1,0), (1,0,1), -(1,0,1), (1,1,1), -(1,1,1)\} \\ &= \{1, -1, i_1, -i_1, i_2, -i_2, i_3, -i_3\}. \end{aligned}$$

Next, we show some properties of the Cayley-Dickson loops.

Theorem 5. *([3]) Any pair of elements of a Cayley-Dickson loop generates a subgroup of the quaternion group. In particular, a pair* x, y *generates a real group when* $x = \pm 1$ *and* $y = \pm 1$*; a complex group when either* $x = \pm 1$*, or* $y = \pm 1$ *(but not both), or* $x = \pm y \neq \pm 1$*; a quaternion group otherwise.*

We denote a loop generated by elements $x_1, \ldots, x_n$ of a loop L by $\langle x_1, \ldots, x_n \rangle$, $n \in \mathbb{N}$.

Definition 6. *A loop L is diassociative if every pair of elements of L generates a group in L.*

Corollary 7. *Cayley-Dickson loop is di-associative.*

Proof. The quaternion group $\mathbb{H}_8$ is associative and the proof follows from Theorem 5. □

Definition 8. *Commutant of a loop L, denoted by $C(L)$, is the set of elements that commute with every element of L. More precisely, $C(L) = \{a \mid ax = xa,\ \forall x \in L\}$.*

Definition 9. *Nucleus of a loop L, denoted by $N(L)$, is the set of elements that associate with all elements of L. More precisely, $N(L) = \{a \mid a \cdot xy = ax \cdot y, xa \cdot y = x \cdot ay, xy \cdot a = x \cdot ya,\ \forall x, y \in L\}$.*

Definition 10. *Center of a loop L, denoted by $Z(L)$, is the set of elements that commute and associate with every element of L. More precisely, $Z(L) = C(L) \cap N(L)$.*

Definition 11. *Let S be a subloop of a loop L. Then S is called a normal subloop if for all $x, y \in L$*

$$xS = Sx,$$
$$(xS)y = x(Sy),$$
$$x(yS) = (xy)S.$$

Definition 12. *Associator subloop of a loop L, denoted by $A(L)$, is the smallest normal subloop of L such that $L/A(L)$ is a group.*

Definition 13. *Derived subloop of a loop L, denoted by L', is the smallest normal subloop of L such that L/L' is an abelian group.*

Lemma 14. *Let S be a subloop of $\mathcal{C}_n$.*

1. *Center of S, $Z(S) = \{1, -1\}$ when $|S| > 4$ and $Z(S) = S$ otherwise.*
2. *Associator subloop of S, $A(S) = Z(S)$ when $|S| > 8$ and $A(S) = 1$ otherwise.*
3. *Derived subloop of S, $S' = Z(S)$ when $|S| > 4$ and $S' = 1$ otherwise.*

Proof.

1. Let S be a subloop of $\mathcal{C}_n$. By Theorem 5, $S \le \mathbb{C}_4$ when $|S| \le 4$; $\mathbb{C}_4$ is an abelian group, hence $Z(S) = S$. Let $|S| > 4$. By Theorem 5, $\langle 1, x \rangle \le \mathbb{C}_4$ and $\langle -1, x \rangle \le \mathbb{C}_4$, $\mathbb{C}_4$ is abelian and therefore $\{1, -1\} \in C(S)$. Let $x \in S \backslash \{\pm 1\}$, choose an element $y \notin \{\pm 1, \pm x\}$. Then $\langle x, y \rangle \cong \mathbb{H}_8$ by Theorem 5, and $[x, y] = -1$. It follows that $C(S) = \{1, -1\}$. Also, $\{1, -1\} \in N(S)$ since $\langle 1, x, y \rangle \le \mathbb{H}_8$ and $\langle -1, x, y \rangle \le \mathbb{H}_8$, therefore $[1, x, y] = 1$ and $[-1, x, y] = 1$ for any $x, y \in S$. It follows that $Z(S) = \{1, -1\}$.
2. Let $|S| > 8$. A group $S/Z(S)$ is abelian, hence $A(S) \le Z(S)$. Also, $A(S) \ne 1$ since S is not a group, so $A(S) = Z(S)$. Let $|S| \le 8$, then $S \le \mathbb{H}_8$ and $\mathbb{H}_8$ is a group, so $A(S) = 1$.
3. Let $|S| > 4$. A group $S/Z(S)$ is abelian, hence $S' \le Z(S)$. Also, $S' \ne 1$ since S is not an abelian group, so $S' = Z(S)$. Let $|S| \le 4$, then $S \le \mathbb{C}_4$ and $\mathbb{C}_4$ is an abelian group, so $S' = 1$. □

Proposition 15. *Let $\mathcal{C}_n$ be a Cayley-Dickson loop.*

1. *Conjugates of the elements of* $\mathcal{C}_n$ *are* $x^* = -x$ *for* $x \in \mathcal{C}_n \setminus \{1,-1\}$, $1^* = 1$, $(-1)^* = -1$.

2. *Orders of the elements of* $\mathcal{C}_n$ *are* $|x| = 4$ *for* $x \in \mathcal{C}_n \setminus \{1,-1\}$, $|1| = 1$, $|-1| = 2$.

3. *Inverses of the elements of* $\mathcal{C}_n$ *are* $x^{-1} = x^*$ *for all* $x \in \mathcal{C}_n$.

4. *Size of* $\mathcal{C}_n$ *is* 2^{n+1}.

5. *For* $k \le n$, $\mathcal{C}_k$ *embeds into* $\mathcal{C}_n$, $k \in \mathbb{N}$.

Proof. 1. By induction on n. In $\mathbb{R}_2$, $1 \cdot 1 = -1 \cdot (-1) = 1$. Suppose $x^* = -x$ holds for all $x \in \mathcal{C}_n \setminus \{\pm 1\}$, then in $\mathcal{C}_{n+1}$ by definition $(x,0)^* = (x^*,0) = (-x,0) = -(x,0)$ and $(x,1)^* = (-x,1) = -(x,1)$.

2. By induction on n. In $\mathbb{C}_4$, $(1,0)(1,0) = (1,0)$ and $(1,1)(1,1) = -(1,0)$. Suppose $x^2 = -1$ holds for all $x \in \mathcal{C}_n \setminus \{\pm 1\}$, then in $\mathcal{C}_{n+1}$ $(x,0)(x,0) = (xx,0) = (-1,0)$ and $(x,1)(x,1) = (-x^*x,0) = (xx,0) = (-1,0)$.

3. Follows from 1. and 2. $x^*x = (-x)x = -(xx) = 1 = -(xx) = x(-x) = xx^*$ when $x \ne \pm 1$ and $(\pm 1)^2 = 1$.

4. By definition.

5. $\mathcal{C}_k \cong \{(x,0) \mid (x,0) \in \mathcal{C}_{k+1}\}$, $k \in \mathbb{N}$. □

Definition 16. *A loop* L *is an inverse property loop if for every* $x \in L$ *there is* $x^{-1} \in L$ *such that* $x^{-1}(xy) = y = (yx)x^{-1}$ *for every* $y \in L$.

Corollary 17. *Cayley-Dickson loop is an inverse property loop.*

Proof. $x^{-1} = x^*$ by Proposition 15. $x^*(xy) = (x^*x)y = y = y(xx^*) = (yx)x^*$ by Corollary 7. □

Definition 18. *Let* L *be a loop. For any* $x, y \in L$ *define commutator* $[x,y]$ *by* $xy = (yx)[x,y]$.

Definition 19. *Let* L *be a loop. For any* $x, y, z \in L$ *define associator* $[x,y,z]$ *by* $xy \cdot z = (x \cdot yz)[x,y,z]$.

Theorem 20. ***(Moufang [7])*** *Let* $(M,\cdot)$ *be a Moufang loop. If* $[x,y,z] = 1$ *for some* $x, y, z \in M$, *then* x, y, z *generate a group in* $(M,\cdot)$.

Lemma 21. *Let* x, y, z *be elements of* $\mathcal{C}_n$.

1. *Commutator* $[x,y] = -1$ *when* $\langle x,y \rangle \cong \mathbb{H}_8$ *and* $[x,y] = 1$ *when* $\langle x,y \rangle < \mathbb{H}_8$.

2. *Associator* $[x,y,z] = 1$ *or* $[x,y,z] = -1$. *In particular,* $[x,y,z] = 1$ *when* $\langle x,y,z \rangle \le \mathbb{H}_8$ *and* $[x,y,z] = -1$ *when* $\langle x,y,z \rangle \cong \mathbb{O}_{16}$.

Proof. 1. By Theorem 5, $\langle x,y \rangle < \mathbb{H}_8$ when either $x = \pm 1$, or $y = \pm 1$, or both, or $x = \pm y$, moreover, $\langle x,y \rangle < \mathbb{H}_8$ implies that $\langle x,y \rangle \le \mathbb{C}_4$. The complex group $\mathbb{C}_4$ is abelian, hence $[x,y] = 1$ when $\langle x,y \rangle < \mathbb{H}_8$. Next, suppose $\langle x,y \rangle \cong \mathbb{H}_8$, i.e., $x \ne \pm 1$, $y \ne \pm 1$, $x \ne \pm y$. The quaternion group $\mathbb{H}_8$ is not abelian, therefore $[x,y] = -1$.

2. By induction on n. Holds on elements of $\mathbb{R}_2$. Suppose $[x,y,z]=1$ or $[x,y,z]=-1$ $\forall x,y,z\in\mathcal{C}_n$. Then in $\mathcal{C}_{n+1}$, $(x,x_{n+1})(y,y_{n+1})\cdot(z,z_{n+1}) = (f(x,y,z),(x_{n+1}+y_{n+1}+z_{n+1}) \bmod 2)$, where $x_{n+1},y_{n+1},z_{n+1}\in\{0,1\}$ and $f(x,y,z)$ is some product of x,y,z,x^*,y^*,z^* and possibly -1. Recall that $x^*=x$ or $x^*=-x$ for $x\in\mathcal{C}_n$, therefore $f(x,y,z)$ is in fact the product of x,y,z, each occuring exactly once, and possibly -1. Similarly, $(x,x_{n+1})\cdot(y,y_{n+1})(z,z_{n+1}) = (g(x,y,z),(x_{n+1}+y_{n+1}+z_{n+1}) \bmod 2)$, where $g(x,y,z)$ is some product of x,y,z, each occuring exactly once, and possibly -1. In other words, $f(x,y,z)$ and $g(x,y,z)$ only differ by a sign, which shows that either

$$[(x,x_{n+1}),(y,y_{n+1}),(z,z_{n+1})]=1 \text{ or } [(x,x_{n+1}),(y,y_{n+1}),(z,z_{n+1})]=-1.$$

Finally, $\mathbb{H}_8$ is associative, therefore $[x,y,z]=1$ when $\langle x,y,z\rangle\le\mathbb{H}_8$.
$\mathbb{O}_{16}$ is a Moufang loop and not a group, therefore by Moufang's Theorem $[x,y,z]=-1$ when $\langle x,y,z\rangle\cong\mathbb{O}_{16}$. □

Remark 22. *A group $\mathcal{C}_n/\{1,-1\}$ is abelian and isomorphic to (multiplicative) $(\mathbb{Z}_2)^n$, where $\mathbb{Z}_2$ is a cyclic group of order 2.*

Proof. Follows from Lemma 14 and construction (4). □

Lemma 23. *Let B be a subloop of $\mathcal{C}_n$.*

1. *If $B\ne 1$ and $x\in\mathcal{C}_n\backslash B$, then $|\langle B,x\rangle| = 2\,|B|$.*
2. *If $B=1$ and $x\in\mathcal{C}_n\backslash B$, then $\langle B,x\rangle=\{1,-1,x,-x\}$.*
3. *Any n elements of a Cayley-Dickson loop generate a subloop of size 2^k, $k\le n+1$.*
4. *The size of B is 2^m for some $m\le n$.*

Proof. 1. Let $1\ne B\le\mathcal{C}_n$ and $x\in\mathcal{C}_n\backslash B$. By Lemma 14, $Z(\mathcal{C}_n)\le B$ and $Z(\mathcal{C}_n)\le\langle B,x\rangle$, then $B/Z(\mathcal{C}_n)$ and $\langle B,x\rangle/Z(\mathcal{C}_n)$ are subgroups of $\mathcal{C}_n/Z(\mathcal{C}_n)\cong(\mathbb{Z}_2)^n$. It follows that $|\langle B,x\rangle/Z(\mathcal{C}_n)| = 2\,|B/Z(\mathcal{C}_n)|$ because we work in the vector space $(\mathbb{Z}_2)^n$ and we added another vector.

2. Let $B=1$. If $x\ne -1$ then $x^2=-1$ by Proposition 15 and $\langle B,x\rangle=\langle x\rangle=\{1,-1,x,-x\}$. Also, $\langle B,-1\rangle=\{1,-1\}$.

3. By induction on n. The size of $\langle x\rangle$ is $1,2$ or 4. Suppose n elements of a Cayley-Dickson loop generate a subloop B of size 2^k for some $k\le n+1$. Add an element x to B. If $x\in B$, then $|\langle B,x\rangle|=|B|=2^k$, $k\le n+1\le n+2$. If $x\notin B$, then $|\langle B,x\rangle| = 2\,|B| = 2^{k+1}$, $k+1\le n+2$, by 1.

4. Follows from 3. □

3 Cayley-Dickson loops are Hamiltonian

Definition 24. *A Hamiltonian loop is a loop in which every subloop is normal.*

Theorem 25. *Cayley-Dickson loop $\mathcal{C}_n$ is Hamiltonian $\forall n\in\mathbb{N}$.*

Proof. Let S be a subloop of $\mathcal{C}_n$, $s \in S$, $x, y \in \mathcal{C}_n$. Using Lemma 21 and Lemma 14,

$$\begin{aligned} xs &= [x,s]sx \in \{sx, -sx\} \subseteq Sx, \\ (xs)y &= [x,s,y]x(sy) \in \{x(sy), -x(sy)\} \subseteq x(Sy), \\ x(ys) &= [x,y,s](xy)s \in \{(xy)s, -(xy)s\} \subseteq (xy)S. \quad \square \end{aligned}$$

Norton [9] formulated a number of theorems characterizing diassociative Hamiltonian loops.

Theorem 26. *(Norton) A Hamiltonian di-associative loop L is either an abelian group, or the direct product of an abelian group with elements of odd order and a loop H with the following properties:*

1. *the commutant of H consists of the elements of order 1 or 2,*
2. *if $x, y, z, \ldots$ are elements not in the commutant, then $x^2 = y^2 = z^2 = \ldots \neq 1$, $x^4 = y^4 = z^4 = \ldots = 1$,*
3. *if x, y do not commute, then $\langle x, y\rangle$ is a quaternion group (since H is assumed not abelian, there exists at least one such pair of elements). If x, y commute, then $x = c_1 y$ where c_1 is an element of the commutant.*
4. *if x, y do not commute and if c_2 is an element of H which commutes with every element of $\langle x, y\rangle$, then c_2 is an element of the commutant.*

Theorem 27. ***(Norton)*** *If A is an abelian group with elements of odd order, T is an abelian group with exponent 2, and K is a di-associative loop such that*

1. *elements of K have order 1, 2 or 4,*
2. *there exist elements x, y in K such that $\langle x, y\rangle \cong \mathbb{H}_8$,*
3. *every element of K of order 2 is in the center,*
4. *if $x, y, z \in K$ are of order 4, then $x^2 = y^2 = z^2$,*
   $xy = d \cdot yx$ where $d = 1$ or $d = x^2$,
   and $xy \cdot z = h(x \cdot yz)$ where $h = 1$ or $h = x^2$,

then their direct product $A \times T \times K$ is a di-associative Hamiltonian loop.

It is showed computationally in [2] that $\mathbb{T}_{64}$ is Hamiltonian. Theorem 27 with $A = T = 1$ can alternatively be used to establish the result for all Cayley-Dickson loops. It is, in fact, used in [9] to show that the octonion loop is Hamiltonian, however, at that time the author did not study the generalized Cayley-Dickson loops.

4 Automorphism groups of Cayley-Dickson loops

Definition 28. *Let L be a loop. A map $\phi : L \mapsto L$ is an automorphism if it is a bijective homomorphism.*

Definition 29. *The set of all automorphisms of a loop L forms a group under composition, called the automorphism group and denoted by $Aut(L)$.*

Definition 30. *Define the orbit of a set X under the action of a group G by $O_G(X) = \{gx \mid g \in G,\ x \in X\}$.*

Definition 31. *Define the (pointwise) stabilizer of a set X in G by $G_X = \{g \in G \mid gx = x,\ x \in X\}$.*

Remark 32. *Recall that $|O_G(X)| = |G : G_X|$.*

We use Remark 32 to find an upper bound on the size of $Aut(\mathbb{C}_4)$ and $Aut(\mathbb{H}_8)$. Let's first consider $G = Aut(\mathbb{C}_4)$. Any automorphism on G fixes 1 and -1, therefore it is only possible for an automorphism to map $i_1 \mapsto i_1$ (e.g., the identity map), and $i_1 \mapsto -i_1$ (e.g., conjugation). The size of the orbit $O_G(i_1)$ is therefore 2. Notice that $G_{\{i_1\}} = G_{\mathbb{C}_4}$, since $\mathbb{C}_4$ is generated by i_1. It follows that

$$|G| = |O_G(i_1)| \cdot \left|G_{\{i_1\}}\right| = |O_G(i_1)| = 2.$$

Next, let $G = Aut(\mathbb{H}_8)$. Again, 1 and -1 are fixed by any automorphism and are not in $O_G(i_1)$, therefore the size of $|O_G(i_1)|$ can be at most $|\mathbb{H}_8| - 2 = 6$. When i_1 is stabilized, $\left|G_{\{i_1\}}\right| = \left|O_{G_{\{i_1\}}}(i_2)\right| \cdot \left|G_{\{i_1,i_2\}}\right|$, moreover, $G_{\{i_1,i_2\}} = G_{\mathbb{H}_8}$, since $\mathbb{H}_8$ is generated by $\{i_1, i_2\}$. The orbit $O_{G_{\{i_1\}}}(i_2)$ can have the size at most $|\mathbb{H}_8| - 4 = 4$, because the set $\{1, -1, i_1, -i_1\}$ is fixed. We have

$$|G| = |O_G(i_1)| \cdot \left|G_{\{i_1\}}\right| = |O_G(i_1)| \cdot \left|O_{G_{\{i_1\}}}(i_2)\right| \cdot \left|G_{\{i_1,i_2\}}\right| = |O_G(i_1)| \cdot \left|O_{G_{\{i_1\}}}(i_2)\right| \le 6 \cdot 4 = 24. \quad (12)$$

It has been shown, in fact, (see, e.g., [10]), that $Aut(\mathbb{H}_8)$ is isomorphic to the symmetric group S_4 of size 24. It has been studied in [6] that $Aut(\mathbb{O}_{16})$ has size 1344 and is a non-split extension of the elementary abelian group $(\mathbb{Z}_2)^3$ of order 8 by the simple group $PSL_2(7)$ of order 168. One can use the approach similar to (12) to see what $Aut(\mathbb{O}_{16})$ looks like. We also calculated the automorphism groups of $\mathbb{S}_{32}$ and $\mathbb{T}_{64}$ using LOOPS package for GAP [8]. Summarizing, the sizes of the automorphism groups of the first five Cayley-Dickson loops are

$$\begin{aligned}
|\mathrm{Aut}\,(\mathbb{C}_4)| &= 2,\\
|\mathrm{Aut}\,(\mathbb{H}_8)| &= 24 = 6 \cdot 4,\\
|\mathrm{Aut}\,(\mathbb{O}_{16})| &= 1344 = 14 \cdot 12 \cdot 8,\\
|\mathrm{Aut}\,(\mathbb{S}_{32})| &= 2688 = 2 \cdot (14 \cdot 12 \cdot 8),\\
|\mathrm{Aut}\,(\mathbb{T}_{64})| &= 5376 = 2 \cdot 2 \cdot (14 \cdot 12 \cdot 8).
\end{aligned}$$

One may notice that the automorphism groups of $\mathbb{C}_4$, $\mathbb{H}_8$ and $\mathbb{O}_{16}$ are as big as they possibly can be, subject to the obvious structural restrictions in $\mathbb{C}_4, \mathbb{H}_8, \mathbb{O}_{16}$, only fixing $\{1, -1\}$. On the contrary, the automorphism groups of $\mathbb{S}_{32}$ and $\mathbb{T}_{64}$ are only double the size of the preceeding ones. Theorem 33 below explains such behavior. We denote $e = (1, 1) \in \mathcal{C}_n$ and use it further in the text.

Theorem 33. *If $\phi : \mathcal{C}_n \mapsto \mathcal{C}_n$ is an automorphism and $\psi = \phi \restriction_{\mathcal{C}_{n-1}}$, where $n \ge 4$, then*

1. $\phi(1) = 1$, $\phi(-1) = -1$,
2. $\phi(e) = e$ *or* $\phi(e) = -e$,
3. $\psi \in Aut(\mathcal{C}_{n-1})$,
4. $\phi((x, 1)) = \psi(x)\phi(e), \forall x \in \mathcal{C}_{n-1}$.

We establish several auxiliary results and use them to prove Theorem 33 at the end of the chapter. The following lemma shows that all subloops of $\mathcal{C}_n$ of size 16 fall into two isomorphism classes. In particular, any such subloop is either isomorphic to $\mathbb{O}_{16}$, the octonion loop, or $\tilde{\mathbb{O}}_{16}$, the quasi-octonion loop, described in [1, 3]. The octonion loop is Moufang, however, the quasi-octonion loop is not. We take $\langle i_1, i_2, i_4\rangle = \pm\{1, i_1, i_2, \dots, i_7\}$ as a canonical octonion loop, and $\langle i_1, i_2, i_{12}\rangle = \pm\{1, i_1, i_2, i_3, i_{12}, i_{13}, i_{14}, i_{15}\}$ as a canonical quasi-octonion loop. We use LOOPS package for GAP [8] in Lemma 34 and further in the text to establish the isomorphisms between the loops we construct, and either $\mathbb{O}_{16}$ or $\tilde{\mathbb{O}}_{16}$.

Lemma 34. *If x, y, z are elements of $\mathcal{C}_n$ such that $|\langle x, y, z\rangle| = 16$, then either*

$$\langle x, y, z\rangle \cong \mathbb{O}_{16} \text{ or } \langle x, y, z\rangle \cong \tilde{\mathbb{O}}_{16}.$$

Proof. Let $x, y, z \in \mathcal{C}_n$. We want to construct a loop $\langle x, y, z\rangle = \pm\{1, x, y, xy, z, xz, yz, (xy)z\}$. Fix the associators $[x, y, z]$, $[x, z, y]$, and $[x, y, xz]$. Using di-associativity and Lemma 21.1,

$$\begin{aligned}
x((xy)z) &= [x,y,z]x(x(yz)) = [x,y,z](xx)(yz) = -[x,y,z]yz, && (13)\\
y(xz) &= -(xz)y = -[x,z,y]x(zy) = [x,z,y]x(yz) = [x,y,z][x,z,y](xy)z, && (14)\\
y((xy)z) &= -((xy)z)y = -[x,y,z](x(yz))y = [x,y,z](x(zy))y \\
&= [x,y,z][x,z,y]((xz)y)y = [x,y,z][x,z,y](xz)(yy) \\
&= -[x,y,z][x,z,y](xz), && (15)\\
(xz)((xy)z) &= -((xy)z)(xz) = -[x,y,z](x(yz))(xz) = [x,y,z](x(zy))(xz) \\
&= [x,y,z][x,z,y]((xz)y)(xz) = -[x,y,z][x,z,y](y(xz))(xz) \\
&= -[x,y,z][x,z,y]y((xz)(xz)) = [x,y,z][x,z,y]y, && (16)\\
(yz)((xy)z) &= [x,y,z](yz)(x(yz)) = -[x,y,z](x(yz))(yz) \\
&= -[x,y,z]x((yz)(yz)) = [x,y,z]x, && (17)
\end{aligned}$$

$$\begin{aligned}
(xy)(xz) &= [x,y,xz]x(y(xz)) = -[x,y,xz]x((xz)y) = -[x,z,y][x,y,xz]x(x(zy)) \\
&= -[x,z,y][x,y,xz](xx)(zy) = [x,z,y][x,y,xz](zy) \\
&= -[x,z,y][x,y,xz](yz). && (18)
\end{aligned}$$

Multiplying (18) by (xy) on the left,

$$(xy)(yz) = [x,z,y][x,y,xz]xz. \qquad (19)$$

Multiplying (18) by (xz) on the right,

$$(yz)(xz) = [x,z,y][x,y,xz]xy. \qquad (20)$$

Equalities (13)-(20) together with some trivial calculations result in Table 1, i.e., it is sufficient to fix $[x, y, z]$, $[x, z, y]$ and $[x, y, xz]$ in order to uniquely define $\langle x, y, z\rangle$. We need to consider the following cases:
If $[x, y, z] = [x, z, y] = [x, y, xz] = -1$, then $\langle x, y, z\rangle \cong \mathbb{O}_{16}$ by $\{x, y, z\} \mapsto \{i_1, i_2, i_4\}$.
If $[x, y, z] = [x, z, y] = -1$, $[x, y, xz] = 1$, then $\langle x, y, z\rangle \cong \tilde{\mathbb{O}}_{16}$ by $\{xz, yz, z\} \mapsto \{i_1, i_2, i_{12}\}$.
If $[x, y, z] = [x, y, xz] = -1$, $[x, z, y] = 1$, then $\langle x, y, z\rangle \cong \tilde{\mathbb{O}}_{16}$ by $\{x, z, y\} \mapsto \{i_1, i_2, i_{12}\}$.

1	x	y	xy	z	xz	yz	(xy)z
x	-1	xy	-y	xz	-z	[x,y,z](xy)z	-[x,y,z]yz
y	-xy	-1	x	yz	[x,y,z][x,z,y](xy)z	-z	-[x,y,z][x,z,y]xz
xy	y	-x	-1	(xy)z	-[x,z,y][x,y,xz]yz	[x,z,y][x,y,xz]xz	-z
z	-xz	-yz	-(xy)z	-1	x	y	xy
xz	z	-[x,y,z][x,z,y](xy)z	[x,z,y][x,y,xz]yz	-x	-1	-[x,z,y][x,y,xz]xy	[x,y,z][x,z,y]y
yz	-[x,y,z](xy)z	z	-[x,z,y][x,y,xz]xz	-y	[x,z,y][x,y,xz]xy	-1	[x,y,z]x
(xy)z	[x,y,z]yz	[x,y,z][x,z,y]xz	z	-xy	-[x,y,z][x,z,y]y	-[x,y,z]x	-1

Table 1: Multiplication table of $\langle x, y, z\rangle$

If $[x,y,z] = -1$, $[x,z,y] = [x,y,xz] = 1$, then $\langle x,y,z\rangle \cong \tilde{\mathbb{O}}_{16}$ by $\{y, -xz, x\} \mapsto \{i_1, i_2, i_{12}\}$.
If $[x,y,z] = 1$, $[x,z,y] = [x,y,xz] = -1$, then $\langle x,y,z\rangle \cong \tilde{\mathbb{O}}_{16}$ by $\{-xy, z, x\} \mapsto \{i_1, i_2, i_{12}\}$.
If $[x,y,z] = [x,y,xz] = 1$, $[x,z,y] = -1$, then $\langle x,y,z\rangle \cong \tilde{\mathbb{O}}_{16}$ by $\{x, y, z\} \mapsto \{i_1, i_2, i_{12}\}$.
If $[x,y,z] = [x,z,y] = 1$, $[x,y,xz] = -1$, then $\langle x,y,z\rangle \cong \tilde{\mathbb{O}}_{16}$ by $\{y, z, x\} \mapsto \{i_1, i_2, i_{12}\}$.
If $[x,y,z] = [x,z,y] = [x,y,xz] = 1$, then $\langle x,y,z\rangle \cong \mathbb{O}_{16}$ by $\{x, -yz, y\} \mapsto \{i_1, i_2, i_{12}\}$. □

Next, we study the associators in $\mathcal{C}_n$. We use the result to prove Lemmas 36 and 37.

Remark 35. *Let $x, y, z \in \mathcal{C}_{n-1}$, then in $\mathcal{C}_n$*

(a) $[(x,0),(y,0),(z,1)] = [x,y][z,y,x]$,

(b) $[(x,0),(y,1),(z,0)] = [x,z][y,x,z][y,z,x]$,

(c) $[(x,0),(y,1),(z,1)] = [x,y][x,z][z,x,y][x,z,y]$,

(d) $[(x,1),(y,0),(z,0)] = [y,z][x,y,z]$,

(e) $[(x,1),(y,0),(z,1)] = [y,x][y,z][z,y,x]$,

(f) $[(x,1),(y,1),(z,0)] = [z,x][z,y][y,x,z][y,z,x]$,

(g) $[(x,1),(y,1),(z,1)] = [x,y][x,z][y,z][z,x,y][x,z,y]$.

Proof. (a) $(x,0)(y,0)\cdot(z,1) = (xy,0)(z,1) = (z\cdot xy, 1) = [x,y](z\cdot yx, 1)$
$= [x,y][z,y,x](zy\cdot x, 1) = [x,y][z,y,x]((x,0)(zy,1)) = [x,y][z,y,x]((x,0)\cdot(y,0)(z,1))$.

(b) $(x,0)(y,1)\cdot(z,0) = (yx,1)(z,0) = (yx\cdot z^*, 1) = [y,x,z](y\cdot xz^*, 1) = [x,z][y,x,z](y\cdot z^*x, 1)$
$= [x,z][y,x,z][y,z,x](yz^*\cdot x, 1) = [x,z][y,x,z][y,z,x]((x,0)(yz^*,1))$
$= [x,z][y,x,z][y,z,x]((x,0)\cdot(y,1)(z,0))$.

(c) $(x,0)(y,1)\cdot(z,1) = (yx,1)(z,1) = (-z^*\cdot yx, 0) = [x,y](-z^*\cdot xy, 0)$
$= [x,y][z,x,y](-z^*x\cdot y, 0) = [x,y][x,z][z,x,y](x(-z^*)\cdot y, 0)$
$= [x,y][x,z][z,x,y][x,z,y](x\cdot(-z^*)y, 0) = [x,y][x,z][z,x,y][x,z,y]((x,0)\cdot(-z^*y,0))$
$= [x,y][x,z][z,x,y][x,z,y]((x,0)\cdot(y,1)(z,1))$.

(d) $(x,1)(y,0)\cdot(z,0) = (xy^*,1)(z,0) = (xy^*\cdot z^*, 1) = [x,y,z](x\cdot y^*z^*, 1)$
$= [x,y,z]((x,1)((y^*z^*)^*, 0)) = [x,y,z]((x,1)(zy,0)) = [y,z][x,y,z]((x,1)(yz,0))$
$= [y,z][x,y,z]((x,1)\cdot(y,0)(z,0))$.

(e) $(x,1)(y,0)\cdot(z,1) = (xy^*,1)(z,1) = (-z^*\cdot xy^*,0) = [y,x](-z^*\cdot y^*x,0)$
$= [y,x][z,y,x](-z^*y^*\cdot x,0) = [y,x][z,y,x]((x,1)(-(-z^*y^*)^*,1))$
$= [y,x][z,y,x]((x,1)(yz,1)) = [y,x][y,z][z,y,x]((x,1)(zy,1))$
$= [y,x][y,z][z,y,x]((x,1)\cdot(y,0)(z,1))$.

(f) $(x,1)(y,1)\cdot(z,0) = (-y^*x,0)(z,0) = (-y^*x\cdot z,0) = [y,x,z](-y^*\cdot xz,0)$
$= [z,x][y,x,z](-y^*\cdot zx,0) = [z,x][y,x,z][y,z,x](-y^*z\cdot x,0)$
$= [z,x][y,x,z][y,z,x]((x,1)(-(-y^*z)^*,1)) = [z,x][y,x,z][y,z,x]((x,1)(z^*y,1))$
$= [z,x][z,y][y,x,z][y,z,x]((x,1)(yz^*,1)) = [z,x][z,y][y,x,z][y,z,x]((x,1)\cdot(y,1)(z,0))$.

(g) $(x,1)(y,1)\cdot(z,1) = (-y^*x,0)(z,1) = (z\cdot(-y^*)x,1) = [x,y](z\cdot x(-y^*),1)$
$= [x,y][z,x,y](zx\cdot(-y^*),1) = [x,y][x,z][z,x,y](xz\cdot(-y^*),1)$
$= [x,y][x,z][z,x,y][x,z,y](x\cdot z(-y^*),1) = [x,y][x,z][z,x,y][x,z,y]((x,1)((z(-y^*))^*,0))$
$= [x,y][x,z][z,x,y][x,z,y]((x,1)(-yz^*,0)) = [x,y][x,z][y,z][z,x,y][x,z,y]((x,1)(-z^*y,0))$
$= [x,y][x,z][y,z][z,x,y][x,z,y]((x,1)\cdot(y,1)(z,1))$. □

Lemma 36 shows that $e\in\mathcal{C}_n$ is special; if we consider a subloop $\langle x,y,e\rangle$ of $\mathcal{C}_n$ such that $|\langle x,y,e\rangle| = 16$, then $\langle x,y,e\rangle$ is always a copy of the octonion loop $\mathbb{O}_{16}$. Lemma 41 shows that this, however, is not the case for any element of $\mathcal{C}_n\backslash\{\pm e\}$. Therefore, an automorphism on $\mathcal{C}_n$ cannot map e to an element $x\in\mathcal{C}_n\backslash\{\pm e\}$. Also, we use Lemma 40 to show that an element $(x,0)$ of $\mathcal{C}_n$ is contained in more copies of $\mathcal{C}_{n-1}$ than an element $(y,1)$, and hence an automorphism on $\mathcal{C}_n$ cannot map $(x,0)$ to $(y,1)$ for any $x,y\in\mathcal{C}_{n-1}$.

Lemma 36. *$\langle x,y,e\rangle\cong\mathbb{O}_{16}$ for any $x,y\in\mathcal{C}_n$ such that $e\notin\langle x,y\rangle\cong\mathbb{H}_8$.*

Proof. Let x,y be elements of $\mathcal{C}_n$ such that $e\notin\langle x,y\rangle\cong\mathbb{H}_8$. As follows from the proof of Lemma 34, in order to prove that $\langle x,y,e\rangle\cong\mathbb{O}_{16}$, it is sufficient to show that

$$[x,y,e] = [x,e,y] = [x,y,xe] = -1. \tag{21}$$

Let $\overline{x},\overline{y}$ be elements of $\mathcal{C}_{n-1}$. We use Remark 35, and consider the following cases:
If $x = (\overline{x},0), y = (\overline{y},0)$, then $xe = (\overline{x},0)(1,1) = (\overline{x},1)$, and

$$\begin{aligned}
[x,y,e] &= [(\overline{x},0),(\overline{y},0),(1,1)] = [\overline{x},\overline{y}][1,\overline{y},\overline{x}] = -1,\\
[x,e,y] &= [(\overline{x},0),(1,1),(\overline{y},0)] = [\overline{x},\overline{y}][1,\overline{x},\overline{y}][1,\overline{y},\overline{x}] = -1,\\
[x,y,xe] &= [(\overline{x},0),(\overline{y},0),(\overline{x},1)] = [\overline{x},\overline{y}][\overline{x},\overline{y},\overline{x}] = -1.
\end{aligned}$$

If $x = (\overline{x},0), y = (\overline{y},1)$, then $xe = (\overline{x},0)(1,1) = (\overline{x},1)$, and

$$\begin{aligned}
[x,y,e] &= [(\overline{x},0),(\overline{y},1),(1,1)] = [\overline{x},\overline{y}][\overline{x},1][1,\overline{x},\overline{y}][\overline{x},1,\overline{y}] = -1,\\
[x,e,y] &= [(\overline{x},0),(1,1),(\overline{y},1)] = [\overline{x},1][\overline{x},\overline{y}][\overline{y},\overline{x},1][\overline{x},\overline{y},1] = -1,\\
[x,y,xe] &= [(\overline{x},0),(\overline{y},1),(\overline{x},1)] = [\overline{x},\overline{y}][\overline{x},\overline{x}][\overline{x},\overline{x},\overline{y}][\overline{x},\overline{x},\overline{y}] = -1.
\end{aligned}$$

If $x = (\overline{x},1), y = (\overline{y},0)$, then $xe = (\overline{x},1)(1,1) = (-\overline{x},0)$, and

$$\begin{aligned}
[x,y,e] &= [(\overline{x},1),(\overline{y},0),(1,1)] = [\overline{y},\overline{x}][\overline{y},1][1,\overline{y},\overline{x}] = -1,\\
[x,e,y] &= [(\overline{x},1),(1,1),(\overline{y},0)] = [\overline{y},\overline{x}][\overline{y},1][1,\overline{x},\overline{y}][1,\overline{y},\overline{x}] = -1,\\
[x,y,xe] &= [(\overline{x},1),(\overline{y},0),(-\overline{x},0)] = [\overline{y},-\overline{x}][\overline{x},\overline{y},-\overline{x}] = -1.
\end{aligned}$$

If $x = (\overline{x}, 1), y = (\overline{y}, 1)$, then $xe = (\overline{x}, 1)(1, 1) = (-\overline{x}, 0)$, and

$$\begin{aligned}
[x, y, e] &= [(\overline{x}, 1), (\overline{y}, 1), (1, 1)] = [\overline{x}, \overline{y}][\overline{x}, 1][\overline{y}, 1][1, \overline{x}, \overline{y}][\overline{x}, 1, \overline{y}] = -1, \\
[x, e, y] &= [(\overline{x}, 1), (1, 1), (\overline{y}, 1)] = [\overline{x}, 1][\overline{x}, \overline{y}][1, \overline{y}][\overline{y}, \overline{x}, 1][\overline{x}, \overline{y}, 1] = -1, \\
[x, y, xe] &= [(\overline{x}, 1), (\overline{y}, 1), (-\overline{x}, 0)] = [-\overline{x}, \overline{x}][-\overline{x}, \overline{y}][\overline{y}, \overline{x}, -\overline{x}][\overline{y}, -\overline{x}, \overline{x}] = -1.
\end{aligned}$$

We conclude that $[x, y, e] = [x, e, y] = [x, y, xe] = -1$ for any $x, y \in \mathcal{C}_n$ such that $e \notin \langle x, y \rangle \cong \mathbb{H}_8$. By Lemma 34, $\langle x, y, e \rangle \cong \mathbb{O}_{16}$ by $\{x, y, e\} \mapsto \{i_1, i_2, i_4\}$. □

The following lemma helps to distinguish between some copies of $\mathbb{O}_{16}$ and $\tilde{\mathbb{O}}_{16}$, and is used to prove Lemmas 40 and 41.

Lemma 37. *Let $x, y, z \in \mathcal{C}_{n-1}$, $n \geq 4$ be such that $\langle x, y, z \rangle \cong \mathbb{O}_{16}$. Then in $\mathcal{C}_n$*

$$\begin{aligned}
\langle (x, 0), (y, 0), (z, 0) \rangle &\cong \langle (x, 1), (y, 1), (z, 1) \rangle \cong \mathbb{O}_{16}, \\
\langle (x, 0), (y, 0), (z, 1) \rangle &\cong \langle (x, 0), (y, 1), (z, 1) \rangle \cong \tilde{\mathbb{O}}_{16}.
\end{aligned}$$

Proof. Let $x, y, z \in \mathcal{C}_{n-1}$ be such that $\langle x, y, z \rangle \cong \mathbb{O}_{16}$. By Lemma 21, $[x, y, z] = [x, z, y] = [y, x, z] = -1$, and $[x, y] = [y, z] = [x, z] = -1$. Using Remark 35,

$$[(x, 0), (z, 1), (y, 0)] = [x, y][z, x, y][z, y, x] = -1 \tag{22}$$

shows that $\langle (x, 0), (y, 0), (z, 1) \rangle > \mathbb{H}_8$ and hence $|\langle (x, 0), (y, 0), (z, 1) \rangle| = 16$, while

$$[(x, 0), (y, 0), (z, 1)] = [x, y][z, y, x] = 1 \tag{23}$$

shows that $\langle (x, 0), (y, 0), (z, 1) \rangle$ is not Moufang and therefore $\langle (x, 0), (y, 0), (z, 1) \rangle \cong \tilde{\mathbb{O}}_{16}$. Similarly, using Remark 35,

$$\begin{aligned}
[(y, 1), (x, 0), (z, 1)] &= [x, y][x, z][z, x, y] = -1, & (24) \\
[(x, 0), (y, 1), (z, 1)] &= [x, y][x, z][z, x, y][x, z, y] = 1 & (25)
\end{aligned}$$

shows that $\langle (x, 0), (y, 1), (z, 1) \rangle \cong \tilde{\mathbb{O}}_{16}$.
A loop $\langle (x, 0), (y, 0), (z, 0) \rangle \cong \mathbb{O}_{16}$ as a copy of $\langle x, y, z \rangle$ in $\mathcal{C}_n$.
A loop $\langle (x, 1), (y, 1), (z, 1) \rangle \cong \mathbb{O}_{16}$ by $\{(x, 1), (y, 1), (z, 1)\} \mapsto \{i_1, i_2, i_4\}$. □

Definition 38. *Let B be a subloop of $\mathcal{C}_n$ of index 2 and D be a subloop of $\mathcal{C}_{n-1}$ of index 2. We call B a subloop of the first type when $B = \mathcal{C}_{n-1}$, a subloop of the second type when $B = D \oplus De$, a subloop of the third type when $B = D \oplus (\mathcal{C}_{n-1} \backslash D)\, e$.*

Figure 1 illustrates all the subloops of index 2 of the sedenion loop $\mathbb{S}_{32}$, each of these subloops being of one of three types. The following lemma shows that this is the case for all Cayley-Dickson loops.

Lemma 39. *If B is a subloop of $\mathcal{C}_n$ of index 2, then B is a subloop of either the first, or the second, or the third type.*

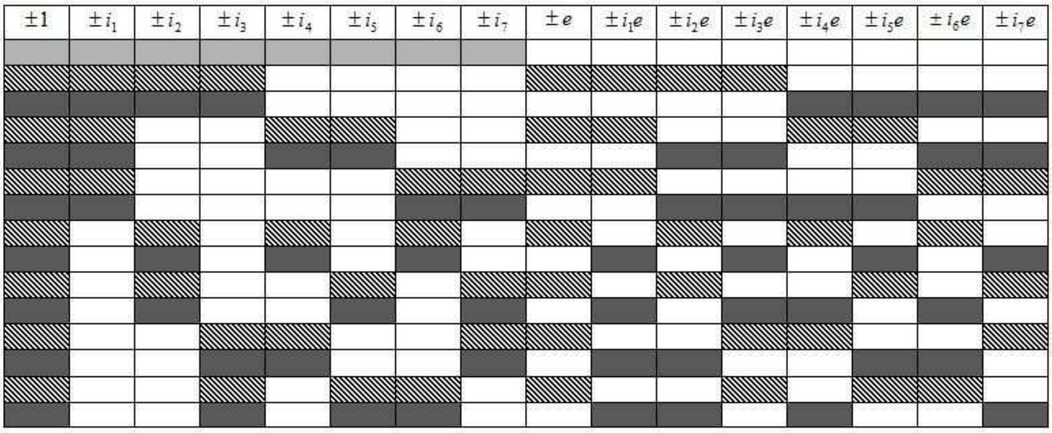

Figure 1: Subloops of $\mathbb{S}_{32}$ of index 2

Proof. By Proposition 15, $\mathcal{C}_{n-1}$ is a subloop of $\mathcal{C}_n$ of index 2, it is of the first type. Let B be a subloop of $\mathcal{C}_n$ of index 2, we assume $B \neq \mathcal{C}_{n-1}$ further in the proof. By Lemma 14, $Z(\mathcal{C}_n) = \{1, -1\} \in B$. Consider $B/Z(\mathcal{C}_n)$ and $\mathcal{C}_n/Z(\mathcal{C}_n)$. By Remark 22, $\mathcal{C}_n/Z(\mathcal{C}_n) \cong (\mathbb{Z}_2)^n$. Also, there is $(a_1, \dots, a_n) \in B/Z(\mathcal{C}_n)$ such that $a_n = 1$, because $B \neq \mathcal{C}_{n-1}$. Define a map $\phi : B/Z(\mathcal{C}_n) \mapsto B/Z(\mathcal{C}_n)$ by $(x_1, \dots, x_n) \mapsto (x_1, \dots, x_n)(a_1, \dots, a_n) = (y_1, \dots, y_n)$, then ϕ maps elements with $x_n = 1$ ($x_n = 0$) to elements with $y_n = 0$ ($y_n = 1$). Hence $B/Z(\mathcal{C}_n)$ contains the same number of elements that end in 0 and that end in 1, and hence a group $\{(x_1, \dots, x_n) \,|\, (x_1, \dots, x_n) \in B, x_n = 0\}$ is a subgroup of $B/Z(\mathcal{C}_n)$ of index 2. This implies that $D = \{\pm(x_1, \dots, x_n) \,|\, (x_1, \dots, x_n) \in B, x_n = 0\}$ is a subloop of B of index 2 and hence D is a subloop of $\mathcal{C}_{n-1}$ of index 2.
Suppose $e \in B$. Define $\psi : B/Z(\mathcal{C}_n) \mapsto B/Z(\mathcal{C}_n)$ by $(x_1, \dots, x_{n-1}, x_n) \mapsto (x_1, \dots, x_{n-1}, x_n)(1, 1) = (x_1, \dots, x_{n-1}, y_n)$. ψ fixes coordinates $x_1, \dots, x_{n-1}$ and maps $x_n = 1$ ($x_n = 0$) to $y_n = 0$ ($y_n = 1$). Therefore when $e \in B$, we see that $B = D \oplus De$, the subloop of the second type.
Now suppose $e \notin B$. Suppose there is an element $(x, 0) \in B/Z(\mathcal{C}_n)$ such that $(x, 0)(1, 1) \in B/Z(\mathcal{C}_n)$. By diassociativity, $(x, 0)((x, 0)(1, 1)) = ((x, 0)(x, 0))(1, 1) = (1, 1) = e \in B/Z(\mathcal{C}_n)$, contradicts the assumption that $e \notin B$. This means that $e \notin B$ implies $B = D \oplus (\mathcal{C}_{n-1} \backslash D)e$, the subloop of the third type. □

Next, we show that, starting at $\mathbb{S}_{32}$, any subloop of $\mathcal{C}_n$ of the third type is not a Cayley-Dickson loop.

Lemma 40. *Let B be a subloop of $\mathcal{C}_n$ of index 2 and D be a subloop of $\mathcal{C}_{n-1}$ of index 2, $n \geq 4$.*

1. *For any $x \in \mathcal{C}_{n-1}$ there exist $y, z \in \mathcal{C}_{n-1}$ such that $\langle x, y, z \rangle \cong \mathbb{O}_{16}$, $\{x, y, z\} \cap D \neq \varnothing$ and $\{x, y, z\} \cap (\mathcal{C}_{n-1} \backslash D) \neq \varnothing$.*

2. *If $e \notin B$ then for any $x \in B$ there exist $y, z \in B$ such that $\langle x, y, z \rangle \cong \tilde{\mathbb{O}}_{16}$.*

3. *If $e \notin B$ then $B \ncong \mathcal{C}_{n-1}$. In particular, any subloop of the third type is not a Cayley-Dickson loop.*

Proof. 1. The size of D is $\frac{|\mathcal{C}_{n-1}|}{2} \geq 8$. Let $e \in \mathcal{C}_{n-1}$. If $x \in D$, choose $y \notin D \cup \langle e, x \rangle$, then $\langle e, x, y \rangle \cong \mathbb{O}_{16}$ by Lemma 36. Similarly, if $x \notin D$, choose $y \in D$, $y \notin \langle e, x \rangle$, then $\langle e, x, y \rangle \cong \mathbb{O}_{16}$ by Lemma 36. If $x = e$, choose $y \notin D \cup \langle e \rangle$ and $z \in D \backslash \langle e, y \rangle$, then $\langle e, x, y \rangle \cong \mathbb{O}_{16}$ by Lemma 36.

2. By Lemma 39, $B = D \oplus (\mathcal{C}_{n-1} \backslash D)\, e$ for some subloop D of $\mathcal{C}_{n-1}$ of index 2. Without loss of generality, suppose $x \in D$. By 1 there exist $y, z \in \mathcal{C}_{n-1}$ such that $\langle x, y, z\rangle \cong \mathbb{O}_{16}$, $\{x, y, z\} \cap D \neq \varnothing$ and $\{x, y, z\} \cap (\mathcal{C}_{n-1} \backslash D) \neq \varnothing$. Again, without loss of generality, suppose $y \in D$ and $z \in \mathcal{C}_{n-1} \backslash D$, therefore $(x, 0), (y, 0), (z, 1) \in B$. Using (22), (23), $\langle (x, 0), (y, 0), (z, 1)\rangle \cong \tilde{\mathbb{O}}_{16}$.

3. By Lemma 36, there is an element $e \in \mathcal{C}_{n-1}$ such that for any $x, y \in \mathcal{C}_{n-1}$, $|\langle e, x, y\rangle| = 16$ implies that $\langle e, x, y\rangle \cong \mathbb{O}_{16}$. However, by 2, B doesn't contain such an element. □

Lemma 41. *Let $x \in \mathcal{C}_n \backslash \{\pm 1, \pm e\}$, $n \geq 4$. There exist $y, z \in \mathcal{C}_n$ such that $\langle x, y, z\rangle \cong \tilde{\mathbb{O}}_{16}$.*

Proof. Without loss of generality, suppose $x \in \mathcal{C}_{n-1}$. By Lemma 40 part 1, there exist $y, z \in \mathcal{C}_{n-1}$ such that $\langle x, y, z\rangle \cong \mathbb{O}_{16}$. Using (22), (23), $\langle (x, 0), (y, 0), (z, 1)\rangle \cong \tilde{\mathbb{O}}_{16}$. □

On $\mathcal{C}_n$, define maps

$$(id, -id) \ : \ (x, x_{n+1}) \mapsto ((-1)^{x_{n+1}} x, x_{n+1}), \tag{26}$$
$$(id, id) \ : \ (x, x_{n+1}) \mapsto (x, x_{n+1}), \tag{27}$$

where $x \in \mathcal{C}_{n-1}$ and $x_{n+1} \in \{0, 1\}$. The map (id, id) is an identity; the map $\phi = (id, -id)$ is an automorphism because

$$\begin{aligned}
\phi((x,0)(y,0)) &= \phi((xy,0)) = (xy,0) = (x,0)(y,0) = \phi((x,0))\phi((y,0)),\\
\phi((x,0)(y,1)) &= \phi((yx,1)) = (-yx,1) = (x,0)(-y,1) = \phi((x,0))\phi((y,1)),\\
\phi((x,1)(y,0)) &= \phi((xy^*,1)) = (-xy^*,1) = (-x,1)(y,0) = \phi((x,1))\phi((y,0)),\\
\phi((x,1)(y,1)) &= \phi((-y^*x,0)) = (-y^*x,0) = (-x,1)(-y,1) = \phi((x,1))\phi((y,1)).
\end{aligned}$$

Proof. (of Theorem 33) Let $\phi : \mathcal{C}_n \mapsto \mathcal{C}_n$, $n \geq 4$, be an automorphism.

1. By Proposition 15, $\phi(1) = 1$, $\phi(-1) = -1$.

2. Let $x \in \mathcal{C}_n \backslash \{\pm 1, \pm e\}$. By Lemma 41, there exist $y, z \in \mathcal{C}_n$ such that $\langle x, y, z\rangle \cong \tilde{\mathbb{O}}_{16}$, however, by Lemma 36, $\langle e, y, z\rangle \cong \mathbb{O}_{16}$ for any $y, z \in \mathcal{C}_n$. Therefore it is only possible that $\phi(e) = e$, which holds when ϕ is an identity map, or $\phi(e) = -e$, which holds when $\phi = (id, -id)$.

3. Consider the subloops of $\mathcal{C}_n$ of index 2. By Lemma 40, any such subloop of the third type is not isomorphic to $\mathcal{C}_{n-1}$. A subloop of the first type (there is only one such subloop) is a copy of $\mathcal{C}_{n-1}$ in $\mathcal{C}_n$ of the form $\{(x, 0) \mid x \in \mathcal{C}_{n-1}\}$. Therefore any element $(x, 0)$ is contained in at least one more copy of $\mathcal{C}_{n-1}$ compared to an element $(y, 1)$. This shows that for every $x \in \mathcal{C}_{n-1}$, $\phi((x, 0)) = (y, 0)$ for some $y \in \mathcal{C}_{n-1}$ and hence $\psi \in Aut(\mathcal{C}_{n-1})$.

4. Let $x \in \mathcal{C}_{n-1}$. Using multiplication formula (5), $xe = (x, 0)(1, 1) = (x, 1)$. If ϕ is an automorphism on $\mathcal{C}_n$, then $\phi((x, 1)) = \phi((x, 0)(1, 1)) = \phi((x, 0))\phi((1, 1)) = \psi(x)\phi(e)$. □

Proposition 42. *([4]) A group G is a direct product of groups H and K, denoted by $G = H \times K$, iff*

1. *H and K are normal subgroups of G,*

2. *$G = HK$,*

3. *$H \cap K = id$, the trivial subgroup of G.*

Finally, we show that, starting at $\mathbb{S}_{32}$, $Aut(\mathcal{C}_n)$ is a direct product of $Aut(\mathcal{C}_{n-1})$ and a cyclic group of order 2.

Theorem 43. *$Aut(\mathcal{C}_n) \cong Aut(\mathcal{C}_{n-1}) \times \mathbb{Z}_2$, where $\mathbb{Z}_2$ is a cyclic group of order 2, $n \geq 4$.*

Proof. Let $G = Aut(\mathcal{C}_n)$, $K = Aut(\mathcal{C}_{n-1})$, $H = \{(id, id), (id, -id)\} \cong \mathbb{Z}_2$, $n \geq 4$.

1. A group K is normal in G because $[G : K] = 2$.
2. Next, show that H is normal in G. Let $g \in G$, $h \in H$. Notice that $g^{-1}hg \in H$ iff $g^{-1}hg \restriction_{\mathcal{C}_{n-1}} = id_{\mathcal{C}_{n-1}}$. Let $x \in \mathcal{C}_{n-1}$, $g = kh_0$, where $k \in K$, $h_0 \in H$.

$$g^{-1}hg(x) = h_0^{-1}k^{-1}hk\underbrace{h_0(x)}_{x} = h_0^{-1}k^{-1}\underbrace{hk(x)}_{k(x)\in\mathcal{C}_{n-1}} = h_0^{-1}\underbrace{k^{-1}k(x)}_{x} = h_0^{-1}(x) = x,$$

   therefore $g^{-1}hg \in H$.
3. Both K and H are normal subgroups of G, therefore $KH \leq G$. Also, $|KH| \geq 2|K| = |G|$, hence $KH = G$.
4. Obviously, $(id, -id) \notin K$ and $H \cap K = id$. □

Acknowledgements We thank Petr Vojtěchovský for numerous discussions and suggestions.

References

[1] R. E. Cawagas. On the structure and zero divisors of the Cayley-Dickson sedenion algebra. *Discuss. Math. Gen. Algebra Appl.*, 24:251–265, 2004.

[2] R. E. Cawagas, A. S. Carrascal, L. A. Bautista, J. P. Sta. Maria, J. D. Urrutia, and B. Nobles. The subalgebra structure of the Cayley-Dickson algebra of dimension 32. arXiv:0907.2047v3.

[3] C. Culbert. Cayley-Dickson algebras and loops. *J. Gen. Lie Theory Appl.*, 1(1):1–17, 2007.

[4] I. N. Herstein. *Abstract Algebra*. Prentice-Hall, 3rd edition, 1995.

[5] A. Hurwitz. Ueber die Composition der quadratischen Formen von beliebig vielen Variabeln (on the composition of quadratic forms of arbitrary many variables) (in German). *Nachr. Ges. Wiss. Gottingen*, pages 309–316, 1898.

[6] M. Koca and R. Koç. Octonions and the group of order 1344. *Tr. J. of Phys.*, 19:304–319, 1995.

[7] R. Moufang. Zur Struktur von Alternativkörpern (in German). *Math. Ann.*, 110:416–430, 1935.

[8] G. P. Nagy and P. Vojtěchovský. LOOPS, Package for GAP 4. Available at http://www.math.du.edu/loops.

[9] D. A. Norton. Hamiltonian loops. *Proc. Amer. Math. Soc.*, 3:56–65, 1952.

[10] H. J. Zassenhaus. *The theory of groups*. Dover, 2nd edition, 1999.