Cayley–Dickson loops and their permutation groups

Jenya Kirshtein

C12 Energy

Third Mile High Conference on Nonassociative Mathematics
University of Denver
August 13, 2013

Cayley–Dickson doubling process

Define a sequence of power-associative algebras over a field F inductively

$$\mathbb{A}_0 = F,\ a^* = a,\ \text{where } a \in F$$
$$\mathbb{A}_n = \{(a, b) \mid a, b \in \mathbb{A}_{n-1}\},\ n \in \mathbb{N}$$

$$\begin{aligned}\text{with multiplication } (a,b)\cdot(c,d) &= (a\cdot c - d^*\cdot b, d\cdot a + b\cdot c^*)\\ \text{addition } (a,b)+(c,d) &= (a+c, b+d)\\ \text{and conjugation } (a,b)^* &= (a^*, -b)\end{aligned}$$

Note: Cayley–Dickson algebras of dimension > 8 are not composition algebras.

Cayley–Dickson loops

Definition

Define **Cayley–Dickson loops** $(Q_n, \cdot)$ inductively

$$\begin{aligned} Q_0 &= \{1, -1\} \\ Q_n &= \{(x,0), (x,1) \mid x \in Q_{n-1}\} \end{aligned}$$

Multiplication

$(x,0)(y,0) = (xy,0)$
$(x,0)(y,1) = (yx,1)$
$(x,1)(y,0) = (xy^*,1)$
$(x,1)(y,1) = (-y^*x,0)$

Conjugation

$(x,0)^* = (x^*,0)$
$(x,1)^* = (-x,1)$

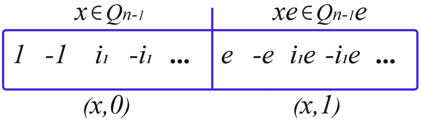
Cayley–Dickson loops are independent of the underlying field F of characteristic not two.
Assume $F = \mathbb{R}$ without loss of generality.

Canonical generators

Definition

Let $e = i_n = (1_{Q_{n-1}}, 1) = (1, \underbrace{0, \ldots, 0}_{n-1}, 1) \in Q_n$, then $Q_n = Q_{n-1} \cup (Q_{n-1} i_n)$, and $Q_n = \langle i_1, i_2, \ldots, i_n \rangle$. We call $i_1, i_2, \ldots, i_n$ **canonical generators** of Q_n.

$$
\begin{aligned}
\textbf{Complex group (abelian) } Q_1 &= \mathbb{C}_4 = \langle i_1 \rangle = \{1, -1, i_1, -i_1\} \\
\textbf{Quaternion group (not abelian) } Q_2 &= \mathbb{H}_8 = \langle i_1, i_2 \rangle = \pm\{1, i_1, i_2, i_1 i_2\} \\
\textbf{Octonion loop (Moufang) } Q_3 &= \mathbb{O}_{16} = \langle i_1, i_2, i_3 \rangle = \\
&= \pm\{1, i_1, i_2, i_1 i_2, i_3, i_1 i_3, i_2 i_3, i_1 i_2 i_3\} \\
\textbf{Sedenion loop (not Moufang) } Q_4 &= \mathbb{S}_{32} = \langle i_1, i_2, i_3, i_4 \rangle
\end{aligned}
$$



Properties

Let $x, y \in Q_n$

- **Conjugate**: $x^* = -x$ for $x \neq \pm 1$, $1^* = 1$, $(-1)^* = -1$
- **Inverse**: $x^{-1} = x^*$
- **Order**: $|x| = 4$ for $x \neq \pm 1$, $|1| = 1$, $|-1| = 2$
- **Size**: $|Q_n| = 2^{n+1}$
- **Embedding**: $(Q_{n-1}, \cdot) < (Q_n, \cdot)$
- **Diassociativity**: any two elements generate a group, $\langle x, y \rangle \leq \mathbb{H}_8$ (quaternion group)
- Q_n **is Hamiltonian**: any subloop S is normal in Q_n
  $xS = Sx, \;\; (xS)y = x(Sy), \;\; x(yS) = (xy)S$

Center, commutators, and associators

Definition

Center of a loop Q, denoted by $Z(Q)$, is the set of elements that commute and associate with every element of Q
Commutator $[x, y]$ is defined by $xy = (yx)[x, y]$
Associator $[x, y, z]$ is defined by $xy \cdot z = (x \cdot yz)[x, y, z]$

Moufang's Theorem

Let Q be a Moufang loop. If $[x, y, z] = 1$ for some $x, y, z \in Q$, then $\langle x, y, z\rangle$ is a group.

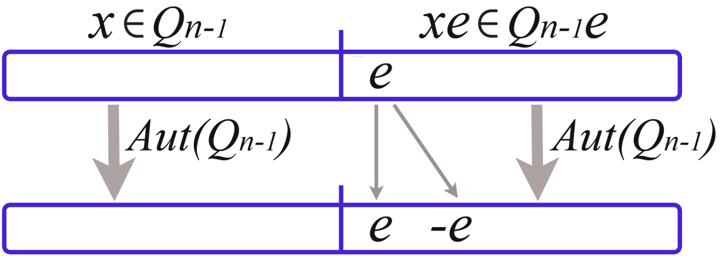
In a **Cayley–Dickson loop** Q_n:
Center $Z(Q_n) = \{1, -1\}$ when $n > 1$, $Z(Q_n) = Q_n$ when $n = 1$.
Commutator $[x, y] = -1$ when $\langle x, y\rangle \cong \mathbb{H}_8$ and $[x, y] = 1$ when $\langle x, y\rangle < \mathbb{H}_8$.
Associator $[x, y, z] = 1$ or $[x, y, z] = -1$. In particular,
$[x, y, z] = 1$ when $\langle x, y, z\rangle \leq \mathbb{H}_8$ and $[x, y, z] = -1$ when $\langle x, y, z\rangle \cong \mathbb{O}_{16}$.

Theorem

$Q_n/\{1, -1\} \cong (\mathbb{Z}_2)^n$.

Automorphism group

	Size observation	**Structure**
$Aut(\mathbb{C}_4)$	2	$\mathbb{Z}_2$
$Aut(\mathbb{H}_8)$	24	$\mathbb{S}_4$
$Aut(\mathbb{O}_{16})$	$1344 = 8 \cdot 168$	Extension of $(\mathbb{Z}_2)^3$ by $PSL_2(7)$
$Aut(\mathbb{S}_{32})$	$2688 = 1344 \cdot 2$	$Aut(\mathbb{O}_{16}) \times \mathbb{Z}_2$
$Aut(\mathbb{T}_{64})$	$5376 = 2688 \cdot 2$	$Aut(\mathbb{S}_{32}) \times \mathbb{Z}_2$
...		
$Aut(Q_n)$	$1344 \cdot 2^{n-3}$	$Aut(Q_{n-1}) \times \mathbb{Z}_2$



Multiplication group and inner mapping group

Definition

Let Q be a loop and $x, a \in Q$. Maps $L_x(a) = xa$ and $R_x(a) = ax$ are **left** and **right translations**. These maps are permutations of Q.

1	2	3	4	5
2	1	5	3	4
3	5	4	2	1
4	3	1	5	2
5	4	2	1	3

L_1	()
L_2	(1,2)(3,5,4)
R_4	(1,4,5)(2,3)
T_3	(4,5)
$L_{2,5}$	(2,4,5,3)
$R_{3,5}$	(2,3)(4,5)

$|Mlt| = 120 = 24 \cdot 5$
$|Inn| = 24$

Definition

Multiplication group $Mlt(Q) = \langle R_x, L_x \mid x \in Q \rangle$
Inner mapping group $Inn(Q) = (Mlt(Q))_1 = \{g \in Mlt(Q) \mid g(1) = 1\}$,
generated by **middle**, **right** and **left inner mappings**
$T_x = R_x L_x^{-1}, \quad L_{x,y} = L_x L_y L_{yx}^{-1}, \quad R_{x,y} = R_x R_y R_{xy}^{-1}$
Size $|Mlt(Q)| = |Q| \cdot |Inn(Q)|$

Inner mapping group

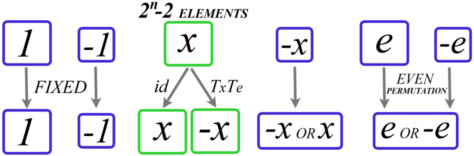
Lemma

Elements of $Mlt(Q_n)$ are even permutations.

$$T_x T_e = (x, -x)(e, -e), \quad x \neq \pm 1$$

Theorem

$Inn(Q_n)$ is an elementary abelian 2-group of order $2^{2^n - 2}$.
Every $f \in Inn(Q_n)$ is a product of disjoint transpositions of the form $(x, -x)$.
$Inn(Q_n) = \langle T_x T_e \mid x \in Q_n, x \neq \pm 1, \pm e \rangle$.

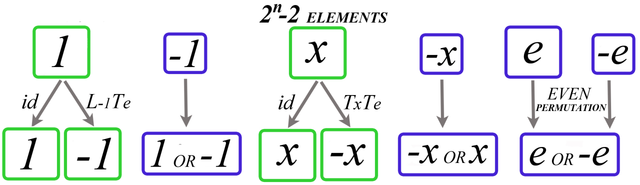


Nonassociative Cayley–Dickson loops are **not automorphic**, i.e., $Inn(Q_n) \not\leq Aut(Q_n)$.

Multiplication group

Theorem

$Mlt(Q_n) \cong (Inn(Q_n) \times Z(Q_n)) \rtimes K.$
$Mlt(Q_n) \cong (\mathbb{Z}_2)^{2^n-1} \rtimes (\mathbb{Z}_2)^n.$



$Inn(Q) \times Z(Q)$

Lemma

$K = \langle L_{i_m}\psi_m \mid i_m$ *canonical generator of* $Q_n, \psi_m \in Inn(Q_n), 1 \leq m \leq n\rangle$
such that $|x| = 2, \forall x \in K.$
Then K *is an elementary abelian* 2*-group of size* 2^n.

Example $Q_3 = \mathbb{O}_{16}$

$$Inn(Q_3) \times Z(Q_3) = \langle L_{-1} T_{i_3}, T_{i_1} T_{i_3}, T_{i_2} T_{i_3}, T_{i_1 i_2} T_{i_3}, T_{i_1 i_3} T_{i_3}, T_{i_2 i_3} T_{i_3}, T_{i_1 i_2 i_3} T_{i_3} \rangle$$

$$K = \langle L_{i_1}\psi_1, L_{i_2}\psi_2, L_{i_3}\psi_3 \rangle$$

$$Mlt(Q_3) \cong (Inn(Q_3) \times Z(Q_3)) \rtimes K$$

$$(n,k)(\tilde{n},\tilde{k}) = (n(k^{-1}\tilde{n}k), k\tilde{k}), \quad n,\tilde{n} \in Inn(Q_3) \times Z(Q_3), \quad k,\tilde{k} \in K$$

$$(k_1)^{-1} \begin{pmatrix} L_{-1} T_{i_3} \\ \hline T_{i_1} T_{i_3} \\ T_{i_2} T_{i_3} \\ T_{i_1 i_2} T_{i_3} \\ \hline T_{i_1 i_3} T_{i_3} \\ T_{i_2 i_3} T_{i_3} \\ T_{i_1 i_2 i_3} T_{i_3} \end{pmatrix} k_1 = \left(\begin{array}{c|ccc|ccc} 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ \hline 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{array}\right) \begin{pmatrix} L_{-1} T_{i_3} \\ \hline T_{i_1} T_{i_3} \\ T_{i_2} T_{i_3} \\ T_{i_1 i_2} T_{i_3} \\ \hline T_{i_1 i_3} T_{i_3} \\ T_{i_2 i_3} T_{i_3} \\ T_{i_1 i_2 i_3} T_{i_3} \end{pmatrix}$$

Table : Action of $k_1 = L_{i_1}\psi_1$ on the basis of $Inn(Q_3) \times Z(Q_3)$

One-sided inner mapping groups

Theorem

$Inn_\ell(Q_n) = Inn_r(Q_n)$.

Proof.

$L_{x,y}(z) = [y,x,z]z, \quad R_{x,y}(z) = [z,x,y]z, \quad [y,x,z] = [z,x,y]$ □

Theorem

$Inn_\ell(Q_n)$ is an elementary abelian 2-group of order $2^{2^{n-1}-1}$.
$Inn_\ell(Q_n) = \left\langle L_{x,e}L_{i_{n-1},e}, h \,\middle|\, 1 \neq x \in Q_{n-1}/\{1,-1\}\right\rangle$.

$$\begin{aligned} L_{x,e}L_{i_{n-1},e} &= (x,-x)(i_{n-1},-i_{n-1})(xe,-xe)(i_{n-1}e,-i_{n-1}e), x \notin \pm\{1,e\} \\ h &= \prod_{z\in(Q_n/\{1,-1\})\setminus(Q_{n-1}/\{1,-1\})} (z,-z) \end{aligned}$$

One-sided multiplication groups

Theorem

Let Q_n be a Cayley–Dickson loop. Then $Mlt_\ell(Q_n) \cong Mlt_r(Q_n)$.

Recall: K is an elementary abelian 2-group of size 2^n.
$K = \langle L_{i_m}\psi_m \mid i_m$ canonical generator of $Q_n, \psi_m \in Inn_\ell(Q_n), 1 \leq m \leq n\rangle$ such that $|x| = 2$, $\forall x \in K$.

Theorem

$Mlt_\ell(Q_n) \cong (Inn_\ell(Q_n) \times Z(Q_n)) \rtimes K$.
$Mlt_\ell(Q_n) \cong (\mathbb{Z}_2)^{2^{n-1}} \rtimes (\mathbb{Z}_2)^n$.

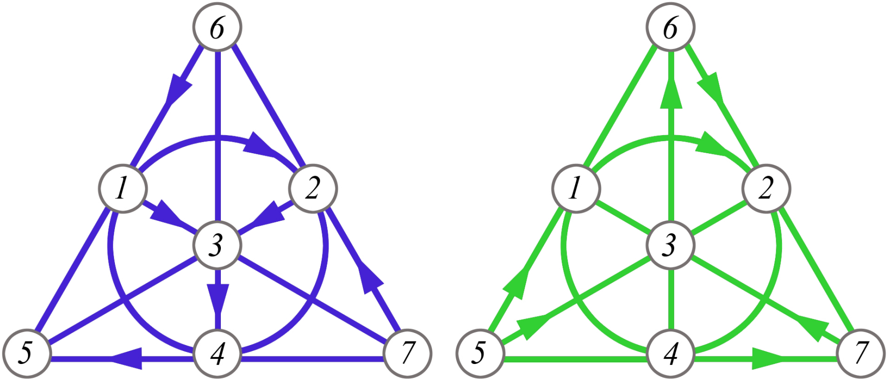
Isomorphism classes of maximal subloops

Size(Q_n)	Max subloops	Isomorphism classes	Representatives
$\mathbb{C}_4$	1	1	$\mathbb{R}_2$
$\mathbb{H}_8$	3	1	$\mathbb{C}_4$
$\mathbb{O}_{16}$	7	1	$\mathbb{H}_8$
$\mathbb{S}_{32}$	15	2	$\mathbb{O}_{16}$ and $\tilde{\mathbb{O}}_{16}$
$\mathbb{T}_{64}$	31	4	$\mathbb{S}_{32}$, $\tilde{\mathbb{S}}^1_{32}$, $\tilde{\mathbb{S}}^2_{32}$, $\tilde{\mathbb{S}}^3_{32}$
Q_{128}	63	8	
Q_{256}	127	16	

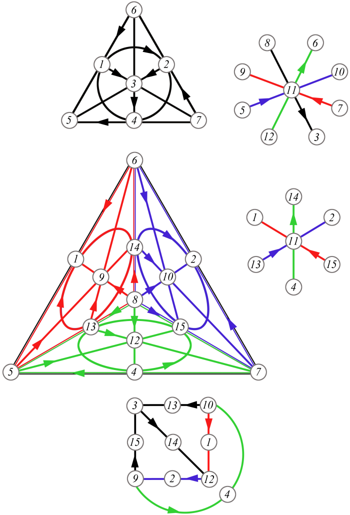
Conjecture

There are 2^{n-3} isomorphism classes of maximal subloops of a Cayley-Dickson loop Q_n.

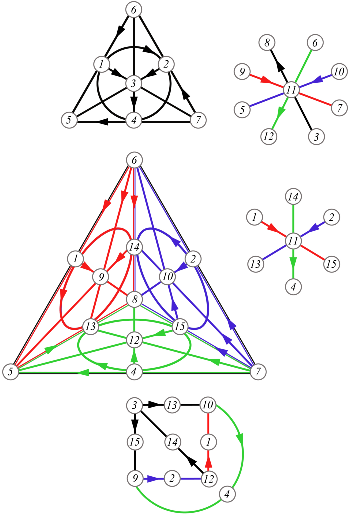
Octonion loop $\mathbb{O}_{16}$ and quasioctonion loop $\tilde{\mathbb{O}}_{16}$



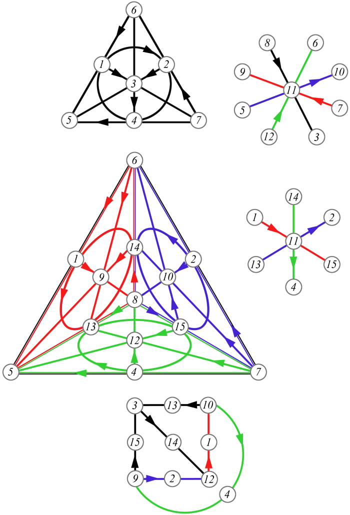
Sedenion loop $\mathbb{S}_{32}$



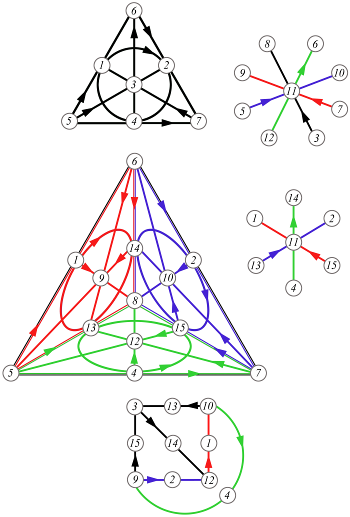
Quasisedenion loop $\tilde{\mathbb{S}}^1_{32}$



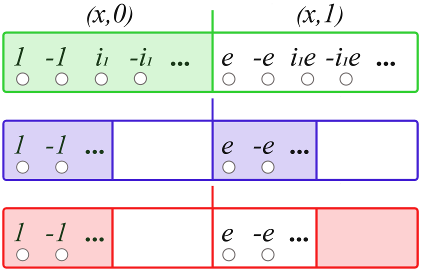
Quasisedenion loop $\tilde{\mathbb{S}}^2_{32}$



Quasisedenion loop $\tilde{\mathbb{S}}^3_{32}$



Maximal subloops



Theorem

Let D be a subloop of Q_{n-1} of index 2. A subloop of Q_n of index 2 is either Q_{n-1},
or $B = D \cup Di_n$,
or $C = D \cup (Q_{n-1} \backslash D)\, i_n$.
$C \not\cong Q_{n-1}$, and $C \not\cong B$.

Associator-commutator calculus

Lemma

In a Cayley–Dickson loop

$$\begin{aligned}[x,y,z] &= [z,y,x],\\ [x,xy,z] &= [x,y,z],\\ [xy,y,xz] &= [y,x,z].\end{aligned}$$

Proof:

$$\begin{aligned} xy\cdot z &= [xy,z]z\cdot xy = [xy,z][x,y]z\cdot yx\\ &= [xy,z][x,y][z,y,x]zy\cdot x\\ &= [xy,z][x,y][z,y,x][x,zy]x\cdot zy\\ &= [xy,z][x,y][z,y,x][x,zy][y,z]x\cdot yz\\ &= [xy,z][x,y][z,y,x][x,zy][y,z][x,y,z]xy\cdot z.\end{aligned}$$

If $\langle x,y,z\rangle$ is a group - done.

Else $[xy,z]=[x,y]=[x,zy]=[y,z]=-1$ - done.

From Q_{n-1} to Q_n

S is a subloop of order 2^n in a Cayley-Dickson loop.
Want to **extend** it to a subloop T of order 2^{n+1} **by adjoining an element** u.
Then $T = S \cup Su$.
The **multiplication** in T **is given by**

$$\begin{aligned} x \cdot y &= xy, \\ x \cdot yu &= [x, y, u](xy)u, \\ xu \cdot y &= [y, xu]y \cdot xu = [y, xu][y, x, u]yx \cdot u = [y, xu][x, y][y, x, u]xy \cdot u, \\ xu \cdot yu &= [y, u]xu \cdot uy = [y, u][x, u, uy]x(u \cdot uy) = -[y, u][x, u, uy]xy \\ &= (\text{note: } [x, u, uy] = [uy, u, x] = [xy, x, u]) = -[y, u][xy, x, u]xy, \end{aligned}$$

where $x, y \in S$.
Need to know associators $[x, y, u]$ for $x, y \in S$.

Subloops of size 16

$|S| = 8$, $S = \pm\{1, a, b, ab\}$. Associators we need to know are:

$$\begin{aligned}
&[a, b, u], \\
&[a, ab, u] = [a, b, u], \\
&[b, a, u], \\
&[b, ab, u] = [b, ba, u] = [b, a, u], \\
&[ab, a, u], \\
&[ab, b, u] = [ab, a, u].
\end{aligned}$$

All we need to describe T are the 3 associators $[a, b, u]$, $[b, a, u]$, $[ab, b, u]$.

Subloops of size 16

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

Lemma (Ginzburg, 1964)

If x, y, z are elements of Q_n such that $|\langle x, y, z\rangle| = 16$, then either

$$\langle x, y, z\rangle \cong \mathbb{O}_{16} \text{ (octonion loop) or}$$
$$\langle x, y, z\rangle \cong \tilde{\mathbb{O}}_{16} \text{ (quasioctonion loop).}$$

Subloops of size 32

Conjecture

Let Q_n be a Cayley-Dickson loop. Every subloop of size 32 of Q_n is isomorphic to a maximal subloop of $\mathbb{T}_{64}$ (the sedenion loop $\mathbb{S}_{32}$, or one of the quasisedenion loops $\tilde{\mathbb{S}}^1_{32}, \tilde{\mathbb{S}}^2_{32}, \tilde{\mathbb{S}}^3_{32}$).

Conjecture

If S is a subloop of a Cayley-Dickson loop Q_n, then S is a maximal subloop of a Cayley-Dickson loop Q_k, $k \leq n+1$.

Subloops of size 32

$|S| = 16$, $S = \langle a, b, c \rangle$, $u \notin S$, $T = S \cup Su$.
To specify T we need $[x, y, u]$,
where $x, y \in S = \pm\{1, a, b, ab, c, ac, bc, (ab)c\}$.
We need:

$[a, b, u]$,
$[a, c, u]$,
$[a, ab, u] = [a, b, u]$,
$[a, ac, u] = [a, c, u]$,
$[a, bc, u]$,
$[a, abc, u] = [a, bc, u]$,
$[b, a, u]$,
$[b, c, u]$,
$[b, ab, u] = [b, a, u]$,
$[b, ac, u]$,
$[ab, ac, u]$,
$[ab, bc, u] = [ab, ac, u]$,
$[ab, abc, u] = [ab, c, u]$,
$[ac, a, u]$,
$[ac, b, u]$,
$[ac, c, u] = [ac, a, u]$,
$[ac, ab, u]$,
$[ac, bc, u] = [ac, ab, u]$,
$[ac, abc, u] = [ac, b, u]$,
$[bc, a, u]$,

Subloops of size 32

$[b, bc, u] = [b, c, u]$,
$[b, abc, u] = [b, ac, u]$,
$[c, a, u]$,
$[c, b, u]$,
$[c, ab, u]$,
$[c, ac, u] = [c, a, u]$,
$[c, bc, u] = [c, b, u]$,
$[c, abc, u] = [c, ab, u]$,
$[ab, a, u]$,
$[ab, b, u] = [ab, a, u]$,
$[ab, c, u]$,
$[bc, b, u]$,
$[bc, c, u] = [bc, b, u]$,
$[bc, ab, u]$,
$[bc, ac, u] = [bc, ab, u]$,
$[bc, abc, u] = [bc, a, u]$,
$[abc, a, u]$,
$[abc, b, u]$,
$[abc, c, u]$,
$[abc, ab, u] = [abc, c, u]$,
$[abc, ac, u] = [abc, b, u]$,
$[abc, bc, u] = [abc, a, u]$.

Future work + References

Future work

- Maximal subloops
- Split Cayley–Dickson loops

References

- Jenya Kirshtein: *Automorphism groups of Cayley–Dickson loops*, Journal of Generalized Lie Theory and Applications, Vol. 6, 2012
- Jenya Kirshtein: *Multiplication groups and inner mapping groups of Cayley–Dickson loops*, Journal of Algebra and Its Applications, Vol. 13, No. 1 (2014)

Thank you!