Investigation of Subalgebra Lattices by Means of Hasse Constants

Petr Vojtěchovský

Abstract. Hasse constants and their basic properties are introduced to facilitate the connection between the lattice of subalgebras of an algebra $C$ and the natural action of the automorphism group $\text{Aut}(C)$ on $C$. These constants are then used to describe the lattice of subloops of the smallest nonassociative simple Moufang loop.

1. Introduction

To completely describe the lattice of subalgebras $\text{Sub}(C)$ of a finite algebra $C$ is a difficult task. Moreover, it is not obvious how to store the information about $\text{Sub}(C)$ efficiently, as the cardinality and complexity of $\text{Sub}(C)$ is typically much larger than that of $C$. Fortunately, sometimes there is a procedure that allows us to calculate the join $A \lor B$ and meet $A \land B$ for every $A, B \in \text{Sub}(C)$. For instance, it is easy to find the join and meet in any boolean algebra $C$, although $|\text{Sub}(C)|$ grows exponentially in $|C|$. It is this ability to calculate $\land$ and $\lor$ that is often understood as a complete description of $\text{Sub}(C)$.

Most of the time we are not so lucky, though, and there is no apparent way to find joins and meets. The main reason is that $A \lor B$ and $A \land B$ can be far from both $A$ and $B$ in the lattice $\text{Sub}(C)$. It is therefore more convenient to have access to a procedure that gives a complete local description of $\text{Sub}(C)$. Assuming that it is possible to find all maximal subalgebras of $A \leq C$ and all subalgebras $B \leq C$ in which $A$ is maximal, the lattice $\text{Sub}(C)$ can be built up inductively. We will refer to all subalgebras immediately above and immediately below $A$ in $\text{Sub}(C)$ as neighbors of $A$, and we denote the set they form by $\text{Nbd}(A)$.

In this context, it is worth paying attention to the automorphism group $\text{Aut}(C)$ and its natural action on $C$, since the neighborhoods of $A$ and $B$ will be “the same” for $A, B \in \text{Sub}(C)$ belonging to the same orbit of transitivity of $\text{Aut}(C)$. Thus, the lattice $\text{Sub}(C)$ can be fully described as long as we find

$(\ell_1)$ one representative $A$ from each orbit of $\text{Aut}(C)$,

$(\ell_2)$ the neighborhood $\text{Nbd}(A)$ for every representative $A$, and

1991 Mathematics Subject Classification: Primary: 06B99, 20N05. Secondary: 17A75, 11H56.

Key words and phrases: Moufang loops, Paige loops, subalgebra lattices, Hasse constants.

While working on this paper the author has been partially supported by Grant Agency of Charles University, grant number 269/2001/B-MAT/MFF.
(ℓ3) an automorphism of C mapping B onto A, for every representative A and
every B from the orbit of A.

To save space, we can store subalgebras by their generating sets, and substitute
Nbd(A) and the automorphisms required by (ℓ3) with an efficient algorithm pro-
ducing those.

The purpose of this paper is twofold. First, to introduce a general tool—Hasse
constants—that is of some help in all three tasks (ℓ1), (ℓ2), (ℓ3). Secondly, to use
Hasse constants to describe the subloop lattice of the smallest nonassociative simple
Moufang loop $M^*(2)$. The investigation of Sub($M^*(2)$) occupies most of this paper,
and is inevitably of rather detailed nature. We maintain that the power of Hasse
constants is sufficiently demonstrated by the fact that Sub($M^*(2)$) was not known
before (see Acknowledgement), especially given the importance of $M^*(2)$ for the
real octonions.

Although considerable invention will be required in each particular case, we be-
lieve that Hasse constants will help to keep track in investigation of any subalgebra
lattice.

A word about the notation: we write $C_n$ for the cyclic group of order $n$, $D_n$ for
the dihedral group of order $2n$, and $E_{2^n}$ for the elementary abelian 2-group of order
$2^n$. A subalgebra generated by the set $S$ well be denoted by $\langle S \rangle$.

2. Hasse constants

Let $A, B, C$ be finite (universal) algebras, $A \leq C$. For $X \leq C$, let $O_X$ denote
the orbit of $X$ under the natural action of Aut(C) on the set of subalgebras of $C$
isomorphic to $X$. We will speak of the subalgebras of $C$ isomorphic to $X$ as copies
of $X$ in $C$. Define

$$H_C(B) = \lvert \{B_0 \leq C; B_0 \cong B\} \rvert,$$
$$H_C(A|B) = \lvert \{B_0 \leq C; A \leq B_0 \cong B\} \rvert.$$

Furthermore, when $B \leq C$, let

$$H^*_C(A|B) = \lvert \{B_0 \leq C; A \leq B_0, B_0 \in O_B\} \rvert.$$

In words, $H_C(B)$ counts the number of copies of $B$ in $C$, $H_C(A|B)$ counts the
number of copies of $B$ in $C$ containing $A$, and $H^*_C(A|B)$ counts the number of
copies of $B$ in $C$ containing $A$ and in the same orbit as $B$.

Yet another description of these constants is perhaps the most appealing. For
$B \leq C$, the constant $H_C(B)$ counts the number of edges connecting $C$ to a copy
of $B$ in the complete Hasse diagram of Sub($C$). The remaining two constants can
be interpreted in a similar way. We will therefore refer to them jointly as Hasse
constants.

Note that $H_C(A|B) = H^*_C(A|B)$ if Aut($C$) acts transitively on the copies of $B$
in $C$.

Lemma 2.1. Let $A, B, C$ be algebras, $A \leq C$.

(i) If $B' \cong B$, $C' \cong C$, then $H_C(B) = H_{C'}(B')$. 


(ii) If $A' \in O_A$, $B' \cong B$, then $\mathcal{H}_C(A|B) = \mathcal{H}_C(A'|B')$.

(iii) If $A' \in O_A$, $B \leq C$, $B' \in O_B$, then $\mathcal{H}_C^*(A|B) = \mathcal{H}_C^*(A'|B')$.

**Proof.** Part (i) is obvious from the definition of $\mathcal{H}_C(B)$. The equality $\mathcal{H}_C(A|B) = \mathcal{H}_C(A'|B')$ holds if $B \cong B'$. Let $A' \in O_A$, and let $f \in \text{Aut}(C)$ be an automorphism mapping $A$ to $A'$. Then $\mathcal{H}_C(A|B) = \mathcal{H}_f(C)(f(A)|f(B)) = \mathcal{H}_C(A'|f(B)) = \mathcal{H}_C(A'|B)$. This proves (ii). Part (iii) is similar (use $O_B = O_{B'}$). □

**Example 2.2.** This example shows that the constants $\mathcal{H}_C(A|B)$, $\mathcal{H}_C(A'|B)$ may differ even though $A \cong A'$. Let $C$ be the group $C_2 \times C_4$, $C_2 = \{0, 1\}$, $C_4 = \{0, 1, 2, 3\}$, and denote by $D = \{0, 2\}$ the two-element subgroup of $C_4$. The lattice of subgroups of $C$ is depicted in Figure 1. With $A = C_1 \times D \cong C_2 \times C_1 = A'$, we have $\mathcal{H}_C(A|C_4) = 2 \neq 0 = \mathcal{H}_C(A'|C_4)$.

![Figure 1. Lattice of subgroups of $C_2 \times C_4$](image)

**Proposition 2.3.** Let $C$ be an algebra, $A, B \leq C$. Let $A_1, \ldots, A_m$ be representatives from all orbits $O_{A_1}, \ldots, O_{A_m}$ of the action of $\text{Aut}(C)$ on the copies of $A$ in $C$. Similarly, let $B_1, \ldots, B_n$ be representatives for $B$. Then

$$
\mathcal{H}_C(A|B) = \sum_{j=1}^{n} \mathcal{H}_C^*(A|B_j), \quad (1)
$$

$$
\mathcal{H}_B(A) \cdot |O_B| = \sum_{i=1}^{m} |O_{A_i}| \cdot \mathcal{H}_C^*(A_i|B), \quad (2)
$$

$$
\mathcal{H}_B(A) \cdot \mathcal{H}_C(B) = \sum_{i=1}^{m} |O_{A_i}| \cdot \mathcal{H}_C(A_i|B). \quad (3)
$$

When $\text{Aut}(C)$ acts transitively on the copies of $B$ (i.e., when $n = 1$), then (2) coincides with (1). When $\text{Aut}(C)$ acts transitively on the copies of $A$ (i.e., when
\( m = 1 \), then
\[
\mathcal{H}_B(A) \cdot |O_B| = \mathcal{H}_C(A) \cdot H^*_C(AB),
\]
\[
\mathcal{H}_B(A) \cdot H_C(B) = \mathcal{H}_C(A) \cdot \mathcal{H}_C(AB).
\]

**Proof.** Since every copy of \( B \) in \( C \) belongs to exactly one orbit \( O_B \), (1) follows.

To establish (2), count twice the cardinality \( t \) of \( \{(A_0, B_0); A \cong A_0 \leq B_0 \in O_B\} \).

On the one hand,
\[
t = \sum_{B_0 \in O_B} \mathcal{H}_B(A) \cdot \sum_{B_0 \in O_B} \mathcal{H}_B(A) = \mathcal{H}_B(A) \cdot |O_B|.
\]

On the other hand,
\[
t = \sum_{A_0 \leq C, A_0 \cong A} \mathcal{H}_C(A_0|B) = \sum_{i=1}^{m} \sum_{A_0 \in O_{A_i}} \mathcal{H}_C(A_0|B) \cdot \sum_{i=1}^{m} |O_{A_i}| \cdot \mathcal{H}_C^*(A_i|B).
\]

The proof of (3) is similar to (2). Just count twice the cardinality of the set \( \{(A_0, B_0); A \cong A_0 \leq B_0 \leq C, B_0 \cong B\} \).

When \( m = 1 \), (1) and (5) follow immediately from (2) and (3), respectively. \( \square \)

### 3. Finite simple Moufang loops and loops of type \( M_{2n}(G, 2) \)

Loops satisfying one of the equivalent *Moufang identities*, for instance the identity
\[
((xy)x)z = x(y(xz)),
\]
are called *Moufang loops* [12]. By a result of Kunen [9], every quasigroup satisfying (6) is a Moufang loop. Obviously, every group is a Moufang loop. Moufang loops are *power associative* (i.e., every 1-generated subloop is a group), in fact *diassociative* (i.e., every 2-generated subloop is a group). Every element \( x \) of a Moufang loop has a (unique) two sided inverse \( x^{-1} \).

Paige [11], Doro [6] and Liebeck [10] showed that there is only one class of nonassociative finite simple Moufang loops, consisting of loops \( M^*(q) \), one for each finite field \( GF(q) \).

These loops are best studied via composition algebras. Following [13], let \( O(q) \) be the unique split octonion algebra over \( GF(q) \). Then \( M^*(q) \) is isomorphic to the multiplicative loop of elements of norm 1 in \( O(q) \) modulo the center. The algebra \( O(q) \) was first constructed by Zorn as follows. Given a prime power \( q \), let \( \cdot \) be the standard dot product and \( \times \) the standard vector product on \( GF(q)^3 \). Then the algebra of *vector matrices*
\[
x = \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \quad (a, b \in GF(q), \alpha, \beta \in GF(q)^3)
\]
with addition defined entry-wise and multiplication governed by
\[
\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix} = \begin{pmatrix} ac + \alpha \cdot \delta & a\gamma + \alpha d - \beta \times \delta \\ \beta c + \delta d + \alpha \times \gamma & \beta \cdot \gamma + \beta d \end{pmatrix}
\]
(7)
is isomorphic to \(O(q)\). The norm on \(O(q)\) coincides with the determinant \(\det x = ab - \alpha \cdot \beta\). The neutral element is
\[
e = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 1 \end{pmatrix},
\]
and every element \(x\) with nonzero norm has inverse
\[
x^{-1} = \frac{1}{\det x} \begin{pmatrix} b & -\alpha \\ -\beta & a \end{pmatrix}.
\]

The order of \(M^*(q)\) is \(q^3(q^4 - 1)\) when \(q\) is even, and \(q^3(q^4 - 1)/2\) when \(q\) is odd [11].

Notably, the loop \(M^*(2)\) has also connections to the standard real (division) octonion algebra. Namely, it is isomorphic to the integral real octonions of norm 1 modulo the center (cf. [5], [14]).

Let us recall loops of type \(M_{2n}(G, 2) = M(G)\), first constructed in [1]. For a group \(G\) of order \(n\), define new multiplication \(\cdot\) on \(G \times C_2\) by
\[
(g, i) \cdot (h, j) = ((g^{(-1)^i}h^{(-1)^j})^{(-1)^i}, i + j).
\]

Then \((G \times C_2, \cdot)\) is a Moufang loop, and we denote it by \(M(G)\). It is nonassociative if and only if \(G\) is nonabelian (cf. [1]).

Write \(M(G) = G \cup Gu\) for some element \(u \in M(G) \setminus G\). Lemma 3.1 (cf. [16, Prop 4.12]) is easy to prove once you realize that
- every element of \(Gu\) is of order 2,
- \(G \cdot G = Gu \cdot Gu = G, G \cdot Gu = Gu \cdot G = Gu\),
- every subloop \(H \not\leq G\) of \(M(G)\) satisfies \(|H \cap G\) = \(|H \cap Gu\).

**Lemma 3.1.** Let \(G\) be a group of order \(n\), and let \(M(G) = G \cup Gu\) be constructed as above.

(i) We have
\[
\mathcal{H}_{M(G)}(C_m) = \begin{cases} \mathcal{H}_G(C_m), & \text{if } m \neq 2, \\ \mathcal{H}_G(C_m) + n, & \text{if } m = 2. \end{cases}
\]

(ii) \(\langle H, gu \rangle \cong E_{2k+1}\) for every \(g \in G, H \leq G, H \cong E_{2k}, k \geq 0\).

(iii) For \(k \geq 1\),
\[
\mathcal{H}_{M(G)}(E_{2k}) = \begin{cases} 0, & \text{if } 2^k \leq n, \\ \mathcal{H}_G(E_{2k}) + \mathcal{H}_G(E_{2k-1}) \cdot n \cdot 2^{1-k}, & \text{otherwise}. \end{cases}
\]

(iv) \(\langle g, hu \rangle \cong S_3\) for every \(g, h \in G\) with \(|g| = 3\).

(v) When \(\mathcal{H}_G(C_3) \neq 0\) and \(\mathcal{H}_G(S_3) = 0\), then \(\mathcal{H}_{M(G)}(G) = 1\).

It was proved in [15] that \(M(G)\) is presented (in the variety of Moufang loops) by
\[
\langle x, y, u; R, u^2 = (xu)^2 = (yu)^2 = ((xy)u)^2 = e \rangle,
\]
(8)
whenever $G$ is a 2-generated group with presentation
\[ \langle x, y; R \rangle. \]
In particular, presentations for the loops $M(S_3)$ and $M(A_4)$ can be obtained from this result.

4. Main goal

We proceed to describe the subloop lattice of $M^*(2)$, guided by steps ($\ell_1$), ($\ell_2$), ($\ell_3$) of Section 1. We fulfill ($\ell_1$) and give reasonable amount of details with respect to ($\ell_2$) and ($\ell_3$). In particular, we calculate all Hasse constants $H_C(B)$, $H_C(A|B)$, $H_C^*(A|B)$, for $A < B \leq C = M^*(2)$.

At several places, the reader will be kindly asked to verify a few details by straightforward, easy calculations. Most of these calculations are reduced to a quick glance into Table 1. The table itself can be checked for accuracy within minutes, using Lemma 7.1. No machine computation is needed.

5. Possible subloops

Fix $F = GF(2)$ and $C = M^*(2)$. It is easy to see that $C$ consists of 120 elements of order 1, 2, 3. More precisely,
\[ x = \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \]
satisfies $|x| = 2$ if and only if $a = b$ and $x \neq e$; and $|x| = 3$ if and only if $a \neq b$. To linearize our notation, we write $x = [\alpha, \beta]_a$ when $|x| = 2$, and $x = \{\alpha, \beta\}_a$ when $|x| = 3$. Since $a$ can be calculated from $\alpha$, $\beta$ when $|x| = 2$, we further simplify involutions to $x = [\alpha, \beta]$. Note that $\{\alpha, \beta\}_a^{-1} = \{\alpha, \beta\}_{1+a}$, where the addition is modulo 2.

Elementary counting reveals that there are 63 involutions and 56 elements of order 3 in $C$. Using the language of Hasse constants, $H_C(C_2) = 63$, $H_C(C_3) = 56/2 = 28$.

Chein classified all nonassociative Moufang loops of order at most 63 [2], and we will call such Moufang loops small. Since $C$ has 120 elements, every proper subloop of $C$ is small and can be found in Chein’s list.

As in [12], we say that a finite loop $L$ has the weak Cauchy property when it contains a subloop of order $p$ for every prime $p$ dividing $|L|$. It has the weak Lagrange property if $|H|$ divides $|L|$ for every $H \leq L$. Finally, $L$ has the strong Cauchy (Lagrange) property if every subloop of $L$ has the weak Cauchy (Lagrange) property.

Since 5 divides $|C|$, $C$ does not have the weak Cauchy property. However, it follows from [2, Ch. XIV] that all small Moufang loops have it. (They also have the strong Lagrange property. If one proves that every $M^*(q)$ has the strong Lagrange property, it will follow that all Moufang loops have it (cf. [4]). As of now, this is an
Corollary 5.1. The order of every proper subloop of $C$ is $2^r3^s$, for some $r, s$.

Lemma 5.2. Let $x, y \in C$, $|x| = |y| = 3$, $y \not\in \langle x \rangle$. Then $\langle x, y \rangle$ contains an involution.

Proof. We may assume that $x = \{\alpha, \beta\}_1$, $y = \{\gamma, \delta\}_1$, for some $\alpha, \beta, \gamma, \delta \in F^3$. Then exactly one of the two elements $xy, x^2y$ is of order 2. □

This means that 9 does not divide the order of any subgroup of $C$. Every group of order 24 contains an element of order at least 4 (the only two nonabelian groups of order 24 with Sylow 2-subgroups isomorphic to $E_8$ are $D_6 \times C_2$ and $A_4 \times C_2$). Hence $|G| \in \{1, 2, 3, 4, 6, 8, 12, 16, 32, 48\}$ for every subgroup $G$ of $C$. It is not obvious, at least to the author, that $C$ contains no subgroups of order 16, necessarily isomorphic to $E_{16}$. It is true, however, and we prove it in Section 14. Hence $|G| = \{1, 2, 3, 4, 6, 8, 12\}$.

Chein concludes in [2, Ch. XII] that every small Moufang loop containing no element of order greater that 3 is necessarily of the form $M(G)$ for some nonabelian group $G$. Thanks to the restrictions on $|G|$, there are only two candidates for $G$, namely $S_3$ (the symmetric group of order 6) and $A_4$ (the alternating group of order 12).

Corollary 5.3. A nontrivial subloop of $C$ is isomorphic to

$$C_2, C_3, E_4, S_3, E_8, A_4, M(S_3) \text{ or } M(A_4).$$

In particular, $C$ has the strong Lagrange property.

All loops listed in (9) actually occur as subloops of $C$, as we shall see.

6. Automorphisms

We construct three kinds of automorphisms of $C$.

Lemma 6.1. Let $f : F^3 \rightarrow F^3$ be a nonsingular linear transformation. Define $\hat{f} : O(2) \rightarrow O(2)$ by

$$\hat{f} \left( \begin{array}{cc} a & \alpha \\ \beta & b \end{array} \right) = \left( \begin{array}{cc} a & f(\alpha) \\ f(\beta) & b \end{array} \right).$$

Then $\hat{f} \in \text{Aut}(O(2))$ if (and only if) $f$ is an automorphism of the Lie algebra $(F^3, +, \times)$.

Proof. Linearity is obvious and the rest follows by straightforward computation using Zorn’s multiplication [7]. □

Identify $\pi \in S_3$ with the linear transformation $F^3 \rightarrow F^3$, $(\alpha_1, \alpha_2, \alpha_3) \mapsto (\alpha_{\pi(1)}, \alpha_{\pi(2)}, \alpha_{\pi(3)})$. By Lemma 6.1, $\hat{\pi} \in \text{Aut}(C)$. To keep the terminology simple, we will call such automorphisms permutations (of coordinates).
Define $\partial : O(2) \to O(2)$ by
\[
\partial \left( \begin{array}{cc} a & \alpha \\ \beta & b \end{array} \right) = \left( \begin{array}{cc} b & \beta \\ \alpha & a \end{array} \right),
\]
and verify that $\partial \in \operatorname{Aut}(O(2))$.

Finally, we focus on conjugations. Not every conjugation in a Moufang loop is an automorphism.

**Lemma 6.2.** Let $Q$ be a simple Moufang loop. For $x \in Q$ define $\gamma_x : Q \to Q$ by $\gamma_x(y) = x^{-1}yx$. Then $\gamma_x$ is a nontrivial automorphism of $Q$ if and only if $|x| = 3$.

**Proof.** By [12, Thm IV.1.6], $\gamma_x$ is a pseudo-automorphism with companion $x^{-3}$. So $\gamma_x$ is an automorphism whenever $|x|$ divides 3.

Conversely, if $\gamma_x$ is a nontrivial automorphism of $Q$, then it must be a pseudo-automorphism with companions $e$ and $x^{-3}$. By [12, Thm IV.1.8], the set of all companions of $\gamma_x$ equals $eN(Q)$, where $N(Q)$ is the nucleus of $Q$. Since $Q$ is simple, we must have $x^{-3} = e$. $\square$

**Remark 6.3.** The conclusion of Lemma 6.1 remains valid over any finite field $GF(q)$, but we then get $\tilde{\pi} \in \operatorname{Aut}(O(q))$, rather than $\hat{\pi} \in \operatorname{Aut}(O(q))$. The map $\partial : O(q) \to O(q)$ defined by (10) is an automorphism if and only if $q$ is even.

7. Subloops isomorphic to $C_2$

The detailed discussion concerning Sub($C$) starts here.

**Lemma 7.1.** Let $x = [\alpha, \beta]_n$, $y = [\gamma, \delta]_m$ be two involutions, $x \neq y$, and let $z = \{\varepsilon, \varphi\}_t$ be an element of order 3 in $C$. Then:

(i) $|xy| = 2$ if and only if $\langle x, y \rangle \cong E_3$ if and only if $\alpha \cdot \delta = \beta \cdot \gamma$,

(ii) $|xy| = 3$ if and only if $\langle x, y \rangle \cong S_3$ if and only if $\alpha \cdot \delta \neq \beta \cdot \gamma$,

(iii) $x$ is contained in a copy of $S_3$,

(iv) every copy of $S_3$ contains an involution of the form $[\_ \_ 0]$, $[\_ \_ \_]$,

(v) $|xz| = 2$ if and only if $\alpha \cdot \varphi + \beta \cdot \varepsilon = n$,

(vi) $z$ is contained in a copy of $S_3$.

**Proof.** The involution $x$ commutes with $y$ if and only if $|xy| = 2$. Since
\[
xy = \left( \begin{array}{cc} nm + \alpha \cdot \delta & \_ \\ \_ & nm + \beta \cdot \gamma \end{array} \right),
\]
parts (i) and (ii) follow. Part (v) is proved similarly.

Let $x = [\alpha, \beta]_n$. Without loss of generality, assume that $\beta \neq 0$. Pick $\gamma, \delta$ so that $\alpha \cdot \delta = 0$, $\beta \cdot \gamma \neq 0$. Then choose $m \in \{0, 1\}$ so that $y = [\gamma, \delta]_m \in C$. Then $\langle x, y \rangle \cong S_3$, and (iii) is proved.

Let $G \leq C$, $G \cong S_3$, and suppose that $x = [\alpha, \beta]_1$, $y = [\gamma, \delta]_1 \in G$, $x \neq y$. Then
\[
xy = \left( \begin{array}{cc} \_ & \_ \\ 1 + \alpha \cdot \delta & \alpha + \gamma + \beta \times \delta \end{array} \right).
Since $|xy| = 3$, we have $\alpha \cdot \delta \neq \beta \cdot \gamma$. In other words, $\alpha \cdot \delta + \beta \cdot \gamma = 1$. Then the third involution $xyx \in G$ equals

$$
\begin{pmatrix}
1 + \alpha \cdot \delta + (\alpha + \gamma) \cdot \beta & \cdots \\
\cdots & \cdots & \cdots \\
\cdots & \cdots & \cdots \\
\cdots & \cdots & \cdots
\end{pmatrix} = 
\begin{pmatrix}
\alpha \cdot \beta & \cdots \\
\cdots & \cdots & \cdots \\
\cdots & \cdots & \cdots \\
\cdots & \cdots & \cdots
\end{pmatrix}.
$$

Now, $\alpha \cdot \beta = 0$ since $\det x = 1$, and we are through with (iv).

Since $\det z \neq 0$, we can assume that the first coordinate of both $\varepsilon$ and $\varphi$ is equal to 1. Then $\alpha = (1, 0, 0)$, $\beta = (0, 0, 0)$ and $n = 1$ make $x = [\alpha, \beta]_n$ into an involution satisfying $|zx| = 2$, by (v). This proves (vi).

Let us write $\alpha_1 \alpha_2 \alpha_3$ for the vector $\alpha = (\alpha_1, \alpha_2, \alpha_3) \in F^3$, and $w(\alpha)$ for $\alpha_1 + \alpha_2 + \alpha_3$ (the weight of $\alpha$).

Introduce $x_0 = [111, 111]$ as the canonical involution of $C$.

Observe that when $x, y$ are two involutions of $C$ generating a subgroup isomorphic to $S_3$ then $\gamma_{yx} \in \text{Aut}(C)$ maps $x$ to $y$.

**Proposition 7.2.** Aut$(C)$ acts transitively on the 63 copies of $C_2$ in $C$.

**Proof.** We show how to map an arbitrary $x = [\alpha, \beta]_n$ onto $x_0$. By Lemma 7.1(iii), $x$ is contained in a copy of $S_3$. Then, by Lemma 7.1(iv) and the observation immediately preceding this Proposition, we can assume that $n = 0$.

Let $r = w(\alpha), s = w(\beta)$. Using $\partial$ from Section 6 we can assume that $r \geq s$. We now fix $y = [100, 100]$ and proceed to transform $x$ into $x'$ so that $x' = x_0$, or $x' = y$, or $\langle x', x_0 \rangle \cong S_3$, or $\langle x', y \rangle \cong S_3$.

When $r \not\equiv s \pmod{2}$, then $\langle x, x_0 \rangle \cong S_3$, by Lemma 7.1(ii). So assume that $r \equiv s$. Since $n = 0$, we have $s > 0$, and thus $(r, s) = (1, 1), (2, 2), (3, 1), (3, 3)$. Every permutation of coordinates can be made into an automorphism of $C$, as we have seen in Section 6. Moreover, $x_0$ is invariant under all such permutations. When $(r, s) = (1, 1)$, transform $x$ into $y$. When $(r, s) = (2, 2)$, transform $x$ into $x' = [110, 011]$, and note that $\langle x', y \rangle \cong S_3$. When $(r, s) = (3, 1)$, transform $x$ into $x' = [111, 001]$, and note again that $\langle x', y \rangle \cong S_3$. Finally, when $(r, s) = (3, 3)$, we have $x = x_0$.

Now, when $\langle x', x_0 \rangle \cong S_3$ or $\langle x', y \rangle \cong S_3$, we can permute the involutions of $C$ so that $x'$ is mapped to $x_0$ or $y$, respectively. Since $x_0 = \gamma_{(001, 101)}(y)$, we are done.

Note that, in spirit of (ξ), the proof of Proposition 7.2 tells us how to construct automorphisms mapping involutions of $C$ onto the representative $x_0$.

8. Subloops Isomorphic to $C_3$ or $S_3$

In this section, we apply Proposition 2.3 for the first time. We have taken advantage of the fact that all permutations and $\partial$ leave $x_0$ invariant. To proceed further, we need additional automorphisms with this property.

Consider $v_0 = \{010, 110\}_0, v_1 = \{001, 101\}_0$, and define $\xi : C \to C$ by $\xi = \gamma_{v_1} \circ \gamma_{v_0}$. Then $\xi \in \text{Aut}(C)$, by Lemma 6.2 and $\xi(x_0) = x_0$. 

**Subalgebras and Hasse Constants**

9
Set $x_1 = [110, 100]$, and let $y_0 = x_0x_1 = \{011, 110\}_1$ be the canonical element of order 3.

**Proposition 8.1.** Aut($C$) acts transitively on the copies of $S_3$ and $C_3$.

**Proof.** Since $\mathcal{H}_{S_3}(C_3) = 1$ and $\mathcal{H}_C(C_3|S_3) > 0$, by Lemma 7.2 (vi), it suffices to prove that Aut($C$) acts transitively on the copies of $S_3$. Let $G \cong S_3$, $G = \langle x, y \rangle$, $|x| = |y| = 2$. By Proposition 7.2 we can assume that $x = x_0$. Write $y = [\alpha, \beta]_n$, $r = w(\alpha)$, $s = w(\beta)$. By Lemma 7.1 we have $r \neq s$. Using $\partial$, we can assume that $r > s$. We are going to transform $y$ into $x_1$.

Assume that $n = 1$. Then $\alpha \cdot \beta = 0$. Taking permutations of coordinates and the possible values of $(r, s)$ into account, we transform $y$ into one of $x_2 = [010, 000]$, $x_3 = [011, 100]$, $x_4 = [111, 000]$, $x_5 = [111, 101]$. With $\xi$ as above, check that all of $\xi(x_2)$, $\xi^{-1}(x_3)$, $\xi(x_4)$ and $\xi^{-1}(x_5)$ have zeros on the diagonal.

We may hence assume that $n = 0$. Then $(r, s) = (2, 1)$, and we are done by permuting coordinates. □

**Lemma 8.2.** $\mathcal{H}_C(C_3|S_3) = 16$, $\mathcal{H}_C(S_3) = 336$, $\mathcal{H}_C(C_3|S_3) = 12$.

**Proof.** Pick an involution $x$. By Proposition 8.1 the number of involutions $y$ satisfying $|xy| = 3$ is independent of $x$. One can then immediately see with $x = [100, 100]$, say, that there are 32 such involutions. As $\mathcal{H}_{S_3}(C_2) = 3$, we get $\mathcal{H}_C(C_3|S_3) = 16$. Then, by (5), $\mathcal{H}_C(S_3) = \mathcal{H}_C(C_2) \cdot \mathcal{H}_C(C_3|S_3) = 336$. Again by (5), $\mathcal{H}_C(C_3|S_3) = \mathcal{H}_{S_3}(C_3) \cdot \mathcal{H}_C(S_3) \cdot \mathcal{H}_C(C_3)^{-1} = 12$. □

Note that Lemma 7.1 allows us to construct all copies of $S_3$ containing $x_0$, and also all copies of $S_3$ containing $y_0$. Note further that we did not have to resort to local analysis to find the value of $\mathcal{H}_C(C_3|S_3)$.

From this moment on, we will pay less attention to $(\ell_2)$ and $(\ell_3)$.

9. Subloops isomorphic to $A_4$

Fix $z_0 = \{110, 100\}_0$, and recall that $\mathcal{H}_{A_4}(C_2) = 3$, $\mathcal{H}_{A_4}(C_3) = 4$.

**Proposition 9.1.** Aut($C$) acts transitively on the 63 copies of $A_4$, and $\mathcal{H}_C(C_3|A_4) = 1$.

**Proof.** Working in $C$, we have $(G, x) \cong S_3$ or $A_4$ for every copy $G$ of $C_3$ and every involution $x$. Since $\mathcal{H}_C(C_3|S_3) = 12$ and $\mathcal{H}_{S_3}(C_2) = 3$, there are 36 involutions $x$ in $G$ such that $(G, x) \cong S_3$. Thus $\mathcal{H}_C(C_3|A_4) = (63 - 36) \cdot \mathcal{H}_{A_4}(C_2)^{-1} = 9$. By (5), $\mathcal{H}_C(A_4) = \mathcal{H}_C(C_3) \cdot \mathcal{H}_C(C_3|A_4) \cdot \mathcal{H}_{A_4}(C_3)^{-1} = 63$.

As for the transitivity, pick $G \cong A_4$. By Proposition 7.2 we can assume that $G = \langle x_0, z \rangle$, for some $z = \{\varepsilon, \varphi\}_0$, with $r = w(\varepsilon)$, $s = w(\varphi)$. Since $|xz| = 3$, we have $r \neq s$, by Lemma 7.1 (v), and may thus assume that $r > s \geq 1$. Then $(r, s) = (2, 1)$ is the only possibility, and $z$ can be transformed to $z_0$ or $z_0^{-1}$. □

Perhaps it would be more natural to look at the copies of $E_4$ now, however, the Klein subgroups of $C$ are exceptional in the sense that Aut($C$) does not act
transitively on them (cf. Section 12). We therefore proceed towards 3-generated subloops instead.

10. Subloops isomorphic to $M(S_3)$

Have a look at Table 1. It lists all involutions of $C$ and their relation to a few chosen elements of $C$.

| $\alpha \setminus \beta$ | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|--------------------------|-----|-----|-----|-----|-----|-----|-----|-----|
| 000                      | 3   | 3   | 2 3 | 3   | 2 3 | 2 2 | 2 2 | 3   |
| 001                      | 3   | 2 2 3 | 2 3 | 3   | 2 3 | 3 | 2 2 2 | 3 |
| 010                      | 3   | 2 1 2 | 3 2 2 | 2 | 2 3 3 | 3 | 2 3 | 3 2 |
| 011                      | 2 2 2 | 3 | 3 2 3 | 3 | 2 2 2 | 3 | 2 3 | 3 2 |
| 100                      | 3   | 2 3 | 2 2 3 | 3 | 2 2 3 | 3 | 3 | 2 3 |
| 101                      | 2 3 | 3 | 3 2 2 | 3 | 1 2 3 | 3 3 | 3 | 2 |
| 110                      | 2 3 | 3 | 2 2 3 | 3 | 2 2 3 | 3 | 2 3 | 3 |
| 111                      | 3 | 2 3 2 | 2 3 3 | 3 | 2 2 2 | 3 | 3 | 3 |

Table 1. Involutions in $M^*(2)$ and their relation to a few elements of $M^*(2)$.

By [1] or [15], $\mathcal{H}_{M(S_3)}(S_3) = 3$. By Lemma 8.1(i), $\mathcal{H}_{M(S_3)}(C_2) = 9$.

Introduce $u_0 = [000, 110]$.

Proposition 10.1. $\mathcal{H}_{C}(S_3|M(S_3)) = 1$. In particular, $\operatorname{Aut}(C)$ acts transitively on the 112 copies of $M(S_3)$.

Proof. In view of Proposition 8.1 it suffices to prove $h = \mathcal{H}_{C}(S_3|M(S_3)) = 1$ and count the copies of $M(S_3)$.

By [8], $M(S_3)$ is presented by $\langle x, y, u; \ x^2 = y^2 = (xy)^3 = u^2 = (xu)^2 = (yu)^2 = ((xy)u)^2 = e \rangle$. Using Lemma 7.1 verify that $x = x_0, y = x_1$ and $u = u_0$ satisfy these presenting relations, i.e., that $h = 1$. 

By [1] or [15], $\mathcal{H}_{M(S_3)}(S_3) = 3$. By Lemma 8.1(i), $\mathcal{H}_{M(S_3)}(C_2) = 9$. 

Introduce $u_0 = [000, 110]$.

Proposition 10.1. $\mathcal{H}_{C}(S_3|M(S_3)) = 1$. In particular, $\operatorname{Aut}(C)$ acts transitively on the 112 copies of $M(S_3)$.

Proof. In view of Proposition 8.1 it suffices to prove $h = \mathcal{H}_{C}(S_3|M(S_3)) = 1$ and count the copies of $M(S_3)$.

By [8], $M(S_3)$ is presented by $\langle x, y, u; \ x^2 = y^2 = (xy)^3 = u^2 = (xu)^2 = (yu)^2 = ((xy)u)^2 = e \rangle$. Using Lemma 7.1 verify that $x = x_0, y = x_1$ and $u = u_0$ satisfy these presenting relations, i.e., that $h = 1$. 

By [1] or [15], $\mathcal{H}_{M(S_3)}(S_3) = 3$. By Lemma 8.1(i), $\mathcal{H}_{M(S_3)}(C_2) = 9$. 

Introduce $u_0 = [000, 110]$.
Let $G$ be a copy of $S_3$. By Proposition 5.1 we can assume that $G = \langle x_0, x_1 \rangle$. According to Table 1 there are 6 involutions $u$ such that $|x_0 u| = |x_1 u| = |(x_0 x_1) u| = 2$ (recall that $x_0 x_1 = y_0$). Since $M_12(G) \setminus G$ consists solely of involutions, we have proved $h \leq 1$.

By (3), $\mathcal{H}_C(M(S_3)) = \mathcal{H}_C(S_3) \cdot \mathcal{H}_C(S_3|M(S_3)) \cdot \mathcal{H}_M(S_3)(S_3)^{-1} = 112$. □

11. Subloops isomorphic to $M(A_4)$

We have $\mathcal{H}_{M(A_4)}(A_4) = 1$ as a special case of Lemma 3.1(v).

Introduce $u_1 = \{001, 001\}$.

Proposition 11.1. $\mathcal{H}_C(A_4|M(A_4)) = 1$. In particular, Aut($C$) acts transitively on the 63 copies of $M(A_4)$.

Proof. In view of Proposition 9.1 it suffices to prove $h = \mathcal{H}_C(A_4|M(A_4)) = 1$ and count the copies of $M(A_4)$.

By (8), $M(A_4)$ is presented by $\langle x, y, u; x^2 = y^3 = (xy)^3 = u^2 = (xyu)^2 = (yu)^2 = ((xy)u)^2 = e \rangle$. Verify that $x = x_0$, $y = z_0$ and $u = u_1$ do the job, hence $h \geq 1$.

Let $G$ be a copy of $A_4$. By Proposition 9.1 we can assume that $G = \langle x_0, z_0 \rangle$. Then $v = z_0^{-1}x_0z_0 \in G$ is an involution. According to Table 1 there are 13 involutions $u$ such that $|x_0 u| = |vu| = 2$. (One of them is $x_0v$.) That is why $h \leq 1$.

By (3), $\mathcal{H}_C(M(A_4)) = \mathcal{H}_C(A_4) \cdot \mathcal{H}_C(A_4|M(A_4)) \cdot \mathcal{H}_{M(A_4)}(A_4)^{-1} = 63$. □

Let us calculate a few more Hasse constants.

Lemma 11.2. We have

\[
\begin{align*}
\mathcal{H}_C(C_2|A_4) &= 3, \mathcal{H}_{M(A_4)}(C_3) = 4, \mathcal{H}_C(C_3|M(A_4)) = 9, \\
\mathcal{H}_{M(S_3)}(C_2) &= 9, \mathcal{H}_C(C_2|M(S_3)) = 16, \mathcal{H}_{M(A_4)}(C_2) = 15, \\
\mathcal{H}_C(C_2|M(A_4)) &= 15, \mathcal{H}_{M(S_3)}(C_3) = 1, \mathcal{H}_C(C_3|M(S_3)) = 4, \\
\mathcal{H}_{M(A_4)}(S_3) &= 16, \mathcal{H}_C(S_3|M(A_4)) = 3.
\end{align*}
\]

Proof. Since $\mathcal{H}_{A_4}(C_2) = 3$, (5) yields $\mathcal{H}_C(C_2|A_4) = 3$. As $\mathcal{H}_{M(G)}(C_m)$ is known (Lemma 3.1), the value of $\mathcal{H}_C(C_m|M(G))$ can be calculated by (5), too.

It remains to find $\mathcal{H}_{M(A_4)}(S_3)$ and $\mathcal{H}_C(S_3|M(A_4))$. Let $M = M(A_4) = G \cup Gu$, where $G \cong A_4$. Every subgroup of $M$ isomorphic to $S_3$ can be written as $\langle x, yu \rangle$ for some $x, y \in G$; $|x| = 3$, and there are exactly six choices of $(x, y)$. Since $\mathcal{H}_{A_4}(C_3) = 4$, we have $\mathcal{H}_{M(A_4)}(S_3) = 2 \cdot 4 \cdot 12/6 = 16$. Consequently, $\mathcal{H}_C(S_3|M(A_4)) = 3$. □

12. Subloops isomorphic to $E_4$

As announced before, we show that Aut($C$) does not act transitively on the copies of $E_4$.

Introduce $u_2 = [100, 010]$.

Lemma 12.1. Let $(x, y)$ be one of the 315 copies of $E_4$ in $C$. Then there is $\varphi \in$ Aut($C$) such that $\varphi(x) = x_0$ and $\varphi(y) \in \{u_1, u_2\}$. 
Proof. Recall that $\mathcal{H}_C(C_2|S_3) = 16$. Therefore, given any involution $x$, there are $63 - 1 - 2 \cdot 16 = 30$ involutions $y$ such that $(x, y) \cong E_4$. Hence, $\mathcal{H}_C(E_4) = 63 \cdot 30/(2 \cdot 3) = 315$.

As always, we may assume that $x = x_0$, $y = [\alpha, \beta]_n$, $w(\alpha) = r$, $w(\beta) = s$, $r \equiv s$, and $r \leq s$. When $(r, s) = (0, 2)$, transform $y$ into $u_0$; if $(r, s) = (1, 1)$, into $u_1$ or $u_2$, depending on $n$; if $(r, s) = (1, 3)$, into $u_3 = [001, 111]$; if $(r, s) = (2, 2)$, into $u_4 = [110, 110]$ or $u_5 = [011, 101]$.

Recall the automorphism $\xi$ from Section 8 and check that $\xi(u_4) = u_1$, $\xi(u_3) = u_2$, $\xi(u_5) = u_3$, $\xi^{-1}(u_5) = \partial(u_0)$. Thus $u_4$ can be transformed into $u_1$, and each of $u_0$, $u_3$, $u_5$ can be transformed into $u_2$. \qed

Assume, for a while, that $\text{Aut}(C)$ acts transitively on the 315 copies of $E_4$. Then, by (5), $\mathcal{H}_C(E_4|A_4) = \mathcal{H}_{A_4}(E_4) \cdot \mathcal{H}_C(A_4) \cdot \mathcal{H}_C(E_4)^{-1} = 1 \cdot 63/315$, a contradiction. Hence, by Lemma 12.1 there are 2 orbits of transitivity $O^+$, with representatives $E_4^+ = \langle x_0, u_1 \rangle$, $E_4^+ = \langle x_0, u_2 \rangle$.

Since $\mathcal{H}_C(E_4|A_4) = 3$, we have $\mathcal{H}_C^+(E_4|A_4)^- = 6/2 = 3$. Then $\mathcal{H}_C^-(E_4|A_4)^- = 12$. By [4], $|O^+| = \mathcal{H}_C(C_2)H^*(C_2E_4^+)^{-1} \cdot \mathcal{H}_C(E_4|A_4)$ and, similarly, $|O^-| = 252$.

By [2], $63 = \mathcal{H}_{A_4}(E_4) \cdot \mathcal{H}_C(A_4) = |O^+| \cdot \mathcal{H}_C(E_4|A_4) + |O^-| \cdot \mathcal{H}_C(E_4|A_4)$, $63 \cdot \mathcal{H}_C(E_4|A_4) = 252 \cdot \mathcal{H}_C(E_4|A_4)$, and each of $E_4$ is contained in $A_4$ if and only if it belongs to $O^+$.

Let us have a look at the relation between $E_4$ and $M(S_3)$.

Lemma 12.2. $\mathcal{H}_C(E_4^+|M(S_3)) = 0$, $\mathcal{H}_C(E_4^-|M(S_3)) = 4$.

Proof. Consider $E_4^+ = \langle x_0, u_1 \rangle$. Assume that there is $G \cong S_3$ such that $E_4^+ \leq M(G)$. Since $\{e, g_0, g_1, g_2\} = E_4^+ \not\leq G$, there is exactly one involution $g_i$ in $G$, say $g_0$. Write $g_i = [\alpha_i, \alpha_i]$ for appropriate vectors $\alpha_i \in F^3$, and note that $\alpha_0 + \alpha_1 = \alpha_2 = 0$.

There is $y = [\gamma, \delta] \in G$ such that $\langle y, g_0 \rangle = G$. Then $\langle yg_0 \rangle = 3$, $\langle yg_1 \rangle = \langle yg_2 \rangle = 2$. By Lemma 7.1 $\gamma \cdot \alpha_i \neq \delta \cdot \alpha_i$, if and only if $i = 0$. Hence $0 = \gamma \cdot (\alpha_0 + \alpha_1 + \alpha_2) \neq \delta \cdot (\alpha_0 + \alpha_1 + \alpha_2) = 0$, a contradiction.

Inevitably, $\mathcal{H}_C(E_4^+|M(S_3)) = 0$. We proceed to calculate $\mathcal{H}_C(E_4^-|M(S_3))$. Since $\mathcal{H}_M(S_3)(E_4) = 9$, by Lemma 5.1 we have $9 \cdot 112 = \mathcal{H}_M(S_3)(E_4) \cdot \mathcal{H}_C(M(S_3)) = |O^+| \cdot \mathcal{H}_C(E_4^+|M(S_3)) + |O^-| \cdot \mathcal{H}_C(E_4^-|M(S_3)) = 63 \cdot 0 + 252 \cdot \mathcal{H}_C(E_4^-|M(S_3))$. \qed

Finally, we have a look at the constants $c^+ = \mathcal{H}_C(E_4^+|M(A_4))$, for $c \in \{+,-\}$.

Lemma 12.3. With the above notation for $c^+$, $c^-$, we have

(i) $(c^+, c^-) \in \{(3, 4), (7, 3), (11, 2), (15, 1), (19, 0)\}$,

(ii) $c^+ \leq 7$,

(iii) $c^- \leq 3$.

Hence $c^+ = 7$ and $c^- = 3$.

Proof. Since $\mathcal{H}_{A_4}(C_2) = 3$ and $\mathcal{H}_{A_4}(E_4) = 1$, we have $\mathcal{H}_{M(A_4)}(E_4) = 19$, by Lemma 3.1. Then yields $19 \cdot 63 = \mathcal{H}_{M(A_4)}(E_4) \cdot \mathcal{H}_C(M(A_4)) = |O^+| \cdot c^+ + |O^-| \cdot c^- = 63c^+ + 252c^- = (c^+ + 4c^-) \cdot 63$. In particular, $c^+ + 4c^- = 19$, and (i) follows.
Let $E_4^+ = \langle x_0, u_1 \rangle$. We are trying to find a group $G \cong A_4$ such that $E_4^+ \leq M(G)$. We look again at the distribution of the 3 involutions $x_0$, $u_1$, $x_0u_1$ in the cosets $G$, $Gu$. There are two possibilities: either $E_4^+ \leq G$, or $|E_4^+ \cap G| = 2$. Suppose that $E_4^+ \leq G$. As $H_{A_4}(E_4) = 1$ and $H_{M(A_4)}(A_4) = 1$, there is at most one subloop $M \cong M(A_4)$ such that $E_4^+ \leq M$ in such a case.

Now suppose that $|E_4^+ \cap G| = 2$. Then $E_4^+ \cap G$ is one of the three 2-element subgroups of $E_4^+$. Let us call it $H$. Since $H_{A_4}(C_2) = 3$ and $H_{M(A_4)}(A_4) = 1$, there are at most 3 subloops $M \cong M_{24}(G)$ such that $H \leq G \leq M$. Because there are three ways to choose $H$ in $E_4^+$, there are at most $3 \cdot 3 = 9$ subloops $M \cong M(A_4)$ such that $E_4^+ \leq M$.

Altogether, $c^+ \leq 1 + 9 = 10$. By (i), $c^+ \leq 7$, and (ii) is finished.

Let $E_4^- = \langle x_0, u_2 \rangle$. We are trying to find a group $G \cong A_4$ such that $E_4^- \leq M_{24}(G)$. Since $H_{C}(E_4^- | M(A_4)) = 0$, the group $E_4^-$ is not contained in $G$, i.e., $|E_4^- \cap G| = 2$. By Proposition 7.2 we can assume that $E_4^- \cap G = \{e, x_0\}$. If there is such a group $G$, there is also an element $y = \{(\gamma_1, \gamma_2, \gamma_3), (\delta_1, \delta_2, \delta_3)\}$, such that $\langle x_0, y \rangle = G \cong A_4$, i.e.,

$$|yx_0| = 3, |yu_2| = 2, |y(x_0u_2)| = 2. \quad (11)$$

By Lemma 9.1, the system of equations (11) is equivalent to

$$\begin{align*}
\delta_1 + \delta_2 + \delta_3 + \gamma_1 + \gamma_2 + \gamma_3 &= 1, \\
\delta_1 + \gamma_2 &= 1, \\
\delta_2 + \gamma_1 &= 1. \quad (12)
\end{align*}$$

In particular, $\gamma_3 + \delta_3 = 1$. There are 4 solutions to (12), namely

$$\begin{pmatrix}
\gamma_1, \gamma_2, \gamma_3 \\
\delta_1, \delta_2, \delta_3
\end{pmatrix} = \begin{pmatrix}
k, k + 1, m \\
k, k + 1, m + 1
\end{pmatrix}, \quad (k, m = 0, 1).$$

This is easy to see since both $(\gamma_1, \gamma_2) = (0, 0), (1, 1)$ lead to $\det y = 0$. Hence, there are at most 8 candidates for $y$ (with $n = 0, 1$). However, if $(x_0, y)$ is isomorphic to $A_4$, then every element of order 3 in $\langle x_0, y \rangle$ must satisfy (12). There are 8 elements of order 3 in $A_4$, and thus there is at most 1 subloop $M(G)$ satisfying all of our restrictions.

Because our choice of $x_0 \in E_4^- \cap G$ was one of three possible choices, we conclude that $c^- = 3$.

Combine (i), (ii), (iii) to get $c^+ = 7, c^- = 3$. \qed

13. Subloops isomorphic to $E_8$

Recall the representatives $E_4^+ = \langle x_0, u_1 \rangle$, $E_4^- = \langle x_0, u_2 \rangle$, and observe that the loop $\langle x_0, u_1, u_2 \rangle$ is a group isomorphic to $E_8$.

Lemma 13.1. $H_{C}(E_4^+ | E_8) = 3, H_{C}(E_4^- | E_8) = 1$.

Proof. Write $d^+ = H_{C}(V_1^+ | E_8)$. We have seen that both $d^+$, $d^-$ are positive. Inspection of Table 1 reveals that there are 12 involutions $y \not\in E_4^+$ such that
\[ |x_0y| = |u_1y| = 2. \] This immediately shows that \( d^+ \leq 3 \). In fact, \( y = [000, 110], [010, 010], [010, 100] \) yield 3 different copies of \( E_8 \). Thus \( d^+ = 3 \).

Yet another inspection of Table 1 shows that there are 12 involutions \( y \notin E_4 \), such that \( |x_0y| = |u_2y| = 2 \). This means that \( d^- \leq 3 \), but we prove more. The group \( E_4 \) is contained in 4 copies of \( M(S_3) \), by Lemma 12.2. Let \( M \) be one of them. We can assume that \( M = G \cup Gu \), where \( G \cong S_3 \), \( x_0 \in G \), \( u_2 = u \). Since \( G \cdot Gu = Gu \), every element \( y \) of \( Gu \) satisfies \( |x_0y| = 2 \). No involution \( y \) of \( G \) satisfies \( |x_0y| = 2 \). Since \( Gu \cdot Gu = G \) and \( H_C(C_2) = 3 \), there are 3 involutions \( y \in Gu \) such that \( |yu| = 2 \). One of them is \( x_0y \). Altogether, \( d^- \leq (12 - (3 - 1) \cdot 4)/4 = 1 \). □

**Lemma 13.2.** Every copy of \( E_8 \) in \( C \) contains a subgroup from \( O^- \).

**Proof.** Note that the proof of Lemma 12.1 implies that \( \langle x_0, y \rangle \in O^+ \) if and only if \( y \) is a permutation of \( u_1 \) or \( u_4 \), i.e., \( y \) is one of the 6 diagonal elements in Table I. Let us denote this set by \( S \).

Let \( E \) be a copy of \( E_8 \) in \( C \). Without loss of generality, \( x_0 \in E \). Assume that \( \langle x_0, y \rangle \in O^+ \) for every \( y \in E \setminus \{ e, x_0 \} \). Then \( E = S \cup \{ e, x_0 \} \). We proceed to show that \( x = [001, 001], y = [100, 100] \in S \) satisfy \( \langle x, y \rangle \in O^- \).

We have carefully chosen the notation so that \( y \) is the same as in the proof of Proposition 7.2. According to the last line of that proof, \( x_0 = \gamma_{\{001,101\},1}(y) \). Using the same automorphism again, we get \( \gamma_{\{001,101\},1}(x) = [001, 000] \). Hence \( \langle x, y \rangle \in O^- \). □

**Proposition 13.3.** The group \( Aut(C) \) acts transitively on the 63 copies of \( E_8 \). Also, \( H_C(E_8|M(A_4)) = 3 \).

**Proof.** Let \( E, E' \) be two subgroups of \( C \) isomorphic to \( E_8 \). Then there are \( G, G' \in O^- \) such that \( G \leq E, G' \leq E' \), by Lemma 13.2. Since \( G, G' \) belong to the same orbit, there is \( \varphi \in Aut(C) \) mapping \( G \) onto \( G' \). As \( H_C(E_4|E_8) = 1 \), \( \varphi \) must map \( E \) onto \( E' \).

By 63 and Lemma 13.1, \( 7 \cdot H_C(E_8) = H_{E_8}(E_4) \cdot H_C(E_8) = |O^+| \cdot d^+ + |O^-| \cdot d^- = 63 \cdot 3 + 1 \cdot 252 = 441 \). Hence, \( H_C(E_8) = 63 \). Consequently, \( 5 \) yields \( H_C(E_8|M(A_4)) = H_{M(A_4)}(E_8) \cdot H_C(M(A_4)) \cdot H_C(E_8)^{-1} = 3 \), and we are finished. □

### 14. Subloop lattice

It is about time to show that \( C \) contains no copies of \( E_{16} \). Assume that \( G \cong E_{16} \) is a subgroup of \( C \). By Proposition 13.3, we can assume that \( \langle x_0, u_1, u_2 \rangle \leq G \). Then there must be at least 8 involutions \( y \) outside \( \langle x_0, u_1, u_2 \rangle \) in \( C \) such that \( |x_0y| = |u_1y| = |u_2y| = 2 \). Previous inspection of Table I provided none, a contradiction.

Let us summarize the results about \( M^*(2) \) obtained in this paper.

**Theorem 14.1.** The smallest 120-element nonassociative simple Moufang loop \( C \) satisfies the strong Lagrange property but not the weak Cauchy property. The following loops (and no other) appear as subloops of \( C \): \( \{ e \}, C_2, C_3, E_4, S_3, E_8, A_4, M(S_3), M(A_4), \) and \( C \).
The automorphism group Aut(C) acts transitively on the copies of each of these subloops, with the exception of $E_4$. There are two orbits of transitivity $O^+$, $O^-$ for $E_4$. With the notational conventions introduced in Section 5, we have the following orbit representatives:

- $\langle x_0 \rangle$ for $C_2$,
- $\langle y_0 \rangle$ for $C_3$,
- $\langle x_0, u_1 \rangle$ for $O^+$,
- $\langle x_0, u_2 \rangle$ for $O^-$,
- $\langle x_0, y_0 \rangle$ for $S_3$,
- $\langle x_0, u_1, u_2 \rangle$ for $E_8$,
- $\langle x_0, z_0 \rangle$ for $A_4$,
- $\langle x_0, y_0, u_0 \rangle$ for $M(S_3)$,
- $\langle x_0, z_0, u_1 \rangle$ for $M(A_4)$,
- $\langle x_0, y_0, u_1 \rangle$ for $M(A_4)$.

The subloop structure and Hasse constants for $C$ are summarized in Figure 2.

15. Acknowledgement

This paper is based on [16, Ch. 5]. Shortly after I finished working on [16], Orin Chein brought my attention to the work of Merlini Giuliani and Polcino Milles [7]. In [7], the authors studied the subloop lattice of $C = M^*(2) = GLL(F_2)$ for the first time, and

- determined $\mathcal{H}_C(C_2)$, $\mathcal{H}_C(C_3)$, and estimated $\mathcal{H}_C(C_2|E_4)$,
- used a result analogous to Lemma 7.1(i), (ii),
- found all possible isomorphism types of subloops of $C$ and listed one example for each type, thus establishing the strong Lagrange property for $C$,
- sketched the relations between isomorphism types of subloops of $C$,

all without proofs. They did not notice that $E_8$ is not a maximal subloop of $C$. I acknowledge that I compared some of my results with [7].

The notion of Hasse constants is new, to my knowledge. The name itself was suggested to me by Jonathan D. H. Smith.

I would also like to thank the reviewer who pointed out that the values of $\mathcal{H}_C(C_3|M(A_4))$ and $\mathcal{H}_C(C_2|M(S_3))$ were in error in the previous version of the paper.

References

[1] O. Chein, Moufang loops of small order I, Trans. Amer. Math. Soc. 188 (1974), 31–51.
[2] O. Chein, Moufang loops of small order, Memoirs of the American Mathematical Society, Volume 13, Issue 1, Number 197 (1978).
[3] O. Chein, H. O. Pflugfelder, The smallest Moufang loop, Arch. Math. 22 (1971), 573–576.
[4] O. Chein, M. Kinyon, A. Rajah, P. Vojtěchovský, Loops and the Lagrange property, to appear in Results in Mathematics.
[5] H. S. M. Coxeter, Integral Cayley numbers, Duke Mathematical Journal 13, no. 4 (1946). Reprinted in H.S.M. Coxeter, Twelve Geometric Essays, Southern Illinois University Press (1968).
[6] S. Doro, Simple Moufang loops, Math. Proc. Camb. Phil. Soc. 83 (1978), 377–392.
Figure 2. The subloop structure and Hasse constants for $M^*(2)$. Two nontrivial representatives $A$, $B$ are connected by an edge if and only if $\mathcal{H}_{M^*(2)}(A|B) > 0$. If $A = \{e\}$ or $B = M^*(2)$, the two representatives $A$, $B$ are connected by an edge if and only if a copy of $A$ is maximal in $B$. The edge connecting $A$ and $B$ is thick if and only if a copy of $A$ is maximal in $B$. The constants $|O_A|$, $\mathcal{H}_B(A)$, $\mathcal{H}^*_{M^*(2)}(A|B)$ are located in the diagram as follows: $|O_A|$ next to $A$; $\mathcal{H}_B(A)$ and $\mathcal{H}^*_{M^*(2)}(A|B)$ in the box on the edge connecting $A$ and $B$, separated by colon.

[7] M. L. Merlini Guiliani, César Polcino Milies, On the structure of the simple Moufang loop $GFF(F_2)$, in Nonassociative algebra and its applications, the fourth international conference, Lecture notes in pure and applied mathematics 211, edited by Roberto Costa, Alexander Grishkov, Henrique Guzzo, Jr., Luiz
[8] G. Glauberman, *On loops of odd order*, J. Algebra 1 (1964), 374–396.
[9] K. Kunen, *Moufang quasigroups*, J. Algebra 183 (1996), no 1, 231–234.
[10] M. W. Liebeck, *The classification of finite simple Moufang loops*, Math. Proc. Cambridge Philos. Soc. 102 (1987), 33–47.
[11] L. Paige, *A class of simple Moufang loops*, Proceedings of the American Mathematical Society 7, issue 3 (1956), 471–482.
[12] H. O. Pflugfelder, *Quasigroups and loops: Introduction*, (Sigma series in pure mathematics; 7), Heldermann Verlag Berlin (1990).
[13] T. A. Springer, F. D. Veldkamp, *Octonions, Jordan algebras, and exceptional groups*, Springer Monographs in Mathematics, Springer Verlag (2000).
[14] P. Vojtěchovský, *Generators of nonassociative simple Moufang loops over finite prime fields*, J. Algebra 241 (2001), 186–192.
[15] P. Vojtěchovský, *The smallest Moufang loop revisited*, submitted.
[16] P. Vojtěchovský, *Finite simple Moufang loops*, Ph.D. thesis, Iowa State University (2001). Available online at www.vojtechovsky.com.

Department of Mathematics, Iowa State University, Ames, IA 50011, U.S.A.
E-mail address: petr@math.du.edu