

Coverings of the smallest Paige loop

Stephen M. Gagola III

Received: 2 June 2010 / Accepted: 30 March 2011 / Published online: 20 April 2011
© Springer Science+Business Media, LLC 2011

Abstract By investigating the construction of the split Cayley generalized hexagon, $H(2)$, we get that there do not exist five distinct hexagon lines each a distance two apart from each other. From this we prove that the smallest Paige loop has a covering number of seven and that its automorphism group permutes these coverings transitively.

Keywords Covering number · Moufang loop · Generalized hexagon · Split Cayley hexagon

1 Introduction

A generalized hexagon is an incidence structure containing lines and vertices where any two elements can be joined by a path containing at most seven elements and there does not exist any n -gon for $n < 6$. Namely, its incidence graph has diameter 6 and girth 12. A generalized hexagon of order (s, t) is one where each vertex is incident with $t + 1$ lines and each line is incident with $s + 1$ vertices. The only examples of finite generalized hexagons of order (q, q) are those associated with the group $G_2(q)$ [3].

A Moufang loop is the generalization of a group that arises when the associative law is replaced by the identity $(xy)(zx) = x((yz)x)$. Clearly, any finite non-cyclic loop can be written as a union of finitely many proper subloops. If G is a loop then we say that the smallest number of subloops needed to cover G is called the *covering number* of G . It was shown by Tomkinson in [13] that there does not exist a group with a covering number of seven. Similarly, he conjectured that there are no groups

S.M. Gagola III (✉)
Department of Mathematics, The University of Arizona, 617 N. Santa Rita Ave, Tucson,
AZ 85721-0089, USA
e-mail: sgagola@math.arizona.edu

with a covering number of eleven. It was Detomi and Lucchini [4] who then showed that it is indeed true that there are no groups whose covering number is eleven. Coverings of groups have been broadly explored and some results have been shown by Foguel and Kappe [5] to also hold for loops.

This brings up the question as to whether or not there exist Moufang loops with covering number seven or eleven. We take a look at split Cayley generalized hexagons, $H(q)$, that one gets from the split Cayley algebras and establish results to help us answer this question. We then prove that even though there does not exist a group with a covering number of seven, there does exist a finite simple Moufang loop, namely a Paige loop, that has seven as its covering number. Moreover, its automorphism group permutes all such coverings, with seven proper subloops, transitively.

2 Generalized hexagons

In this section, we establish some concepts about a hexagonal structure that arises from the split octonions. This is the generalized hexagon, sometimes called the Cayley hexagon, which plays a big role in both deriving the covering number of the smallest Paige loop and determining its possible coverings.

A Paige loop is an example of a Moufang loop arising from a split octonion algebra. For an arbitrary field F , let C be the following set of Zorn’s vector matrices:

$$\left\{ \begin{pmatrix} a & \vec{v} \\ \vec{u} & b \end{pmatrix} \mid a, b \in F, \vec{u}, \vec{v} \in F^3 \right\}.$$

Here C is the unique split octonion algebra over the field F where addition and multiplication are defined by

$$\begin{pmatrix} a & \vec{v} \\ \vec{u} & b \end{pmatrix} + \begin{pmatrix} c & \vec{\alpha} \\ \vec{\beta} & d \end{pmatrix} = \begin{pmatrix} a + c & \vec{v} + \vec{\alpha} \\ \vec{u} + \vec{\beta} & b + d \end{pmatrix}$$

and

$$\begin{pmatrix} a & \vec{v} \\ \vec{u} & b \end{pmatrix} \begin{pmatrix} c & \vec{\alpha} \\ \vec{\beta} & d \end{pmatrix} = \begin{pmatrix} ac + \vec{v} \cdot \vec{\beta} & a\vec{\alpha} + d\vec{v} - \vec{u} \times \vec{\beta} \\ b\vec{\beta} + c\vec{u} + \vec{v} \times \vec{\alpha} & bd + \vec{u} \cdot \vec{\alpha} \end{pmatrix},$$

where $\vec{u} \cdot \vec{v}$ and $\vec{u} \times \vec{v}$ are the usual dot product and cross product. With the quadratic form

$$f \left(\begin{pmatrix} a & \vec{v} \\ \vec{u} & b \end{pmatrix} \right) = ab - \vec{v} \cdot \vec{u}$$

C is the split octonion algebra over F where $x \in C$ is nonsingular, namely invertible, if and only if $f(x) \neq 0$. For all $x, y \in C$, the quadratic form admits composition

$$f(xy) = f(x)f(y)$$

and the associated bilinear form for f

$$(x, y) = f(x + y) - f(x) - f(y)$$

is nondegenerate. Thus C is an example of a composition algebra. One can show that, under multiplication, C satisfies the Moufang identities. Therefore, the set of all invertible elements of C , called the general linear loop and denoted by $GLL(F)$, is a Moufang loop. The loop $GLL(F)$ contains a subloop $SLL(F)$, called the special linear loop, consisting of all the elements of norm one where the norm is the quadratic form given above. It was M. Liebeck [10] who classified all of the finite simple nonassociative Moufang loops showing that these were the finite Paige loops, namely, $P(q) = SLL(q)/\{\pm I\}$ where I is the multiplicative identity of C . Note that $P(2) \cong SLL(2)$. Furthermore, the automorphism group of the Paige loop is

$$\begin{aligned} \text{Aut}(P(q)) &= \text{Aut}(C) \\ &= G_2(q). \end{aligned}$$

Definition 2.1 For an algebra C we say that the stabilizer of a subspace $U \subseteq C$ is the subspace $\text{Stab}_C(U) = \{x \in C \mid xu \in U \text{ for all } u \in U\}$.

For a subspace $U \subseteq C$ we will denote the set of all invertible elements of U as U^* .

One can better understand a split octonion algebra by looking at the hexagonal structure that arises from it. A hexagonal structure is an incidence structure containing lines and vertices where any two elements can be joined by a path containing at most seven elements and there does not exist any 2, 3, 4, or 5-gons. If v_1 and v_2 are two such vertices then we will denote the length of the shortest path between v_1 and v_2 by $d(v_1, v_2)$. For an octonion algebra, a *hexagon line* is a totally singular 2-space, which is orthogonal to I , such that the product of any two of its elements is zero. Likewise, a *vertex* is a singular 1-space, orthogonal to I , such that the product of any two of its elements is zero. Here $\text{Aut}(C) = G_2(q)$ is transitive on the set of hexagon lines in C and is also transitive on the set of vertices in C (see [11]). We say that a vertex v is incident to a hexagon line h if v is a subset of h . This induces a hexagonal structure which we call a *generalized hexagon*; see [11] for more details.

Since $\text{Aut}(C) = G_2(q)$ is transitive on the set of hexagon lines in C , one can easily show that if U is a hexagon line in C then

$$\begin{aligned} \text{Stab}_C(U) &= \{x \in C \mid xu \in U \text{ for all } u \in U\} \\ &= \{x \in C \mid ux \in U \text{ for all } u \in U\}. \end{aligned}$$

Let C be a split octonion algebra over F_2 consisting of Zorn’s vector matrices and let M be a maximal subloop of $SLL(F_2) = GLL(F_2)$. Then from [6], M is one of the following:

1. $M = (h^\perp)^* = \text{Stab}_C(h)^*$ for some hexagon line $h \subseteq C$;
2. $M = (Q \cup Q^\perp)^*$ for some quaternion subalgebra $Q \subseteq C$.

These can be described using Chein loops.

Definition 2.2 If G is a group and u is an element that is not in G then one can extend the binary operation from G to $G \cup Gu$ such that:

$$g_1(g_2u) = (g_2g_1)u,$$

$$(g_1u)g_2 = (g_1g_2^{-1})u,$$

$$(g_1u)(g_2u) = g_2^{-1}g_1,$$

for any elements $g_1, g_2 \in G$. Under this binary operation, the set $G \cup Gu$ is a Moufang loop which is called a Chein loop, originally discovered by O. Chein [2], and is usually denoted by $M_{2n}(G, 2)$ where $n = |G|$.

One should note that a maximal subloop of the form $M = \text{Stab}_C(h)^*$ for some hexagon line $h \subseteq C$ is isomorphic to the Chein loop $M_{24}(A_4, 2)$. Also, a maximal subloop of the form $M = (Q \cup Q^\perp)^*$ for some quaternion subalgebra $Q \subseteq C$ is isomorphic to $M_{12}(S_3, 2)$.

We will denote the set of hexagon lines in C over F_2 by H . Likewise we will denote the set of vertices in C by P . Here the number of totally singular 1-spaces of C which are orthogonal to I with multiplication of zero is $|P| = 63$.

Lemma 2.3 *If $h \in H$ and $v \in P$ then h contains exactly three vertices and the number of hexagon lines incident to v is $\deg(v) = 3$.*

Proof See [3, 12]. □

Definition 2.4 The distance between two hexagon lines $h_1, h_2 \in H$, denoted by $d(h_1, h_2)$, is half of the distance in the incidence graph. Furthermore, we say that the hexagon lines $h_1, h_2 \in H$ are adjacent to each other if $d(h_1, h_2) = 1$.

Lemma 2.5 *If $h_1, h_2, h_3 \in H$ such that $d(h_i, h_j) = 2$ for all $i \neq j$ then either*

- (1) h_1, h_2 , and h_3 are contained in a hexagon; or
- (2) h_1, h_2 , and h_3 are all adjacent to some hexagon line $l \in H$.

3 The covering number of $P(2)$

In this section, we will determine the covering number of $P(2)$ and give an example of such a covering. One can easily see that when determining the covering number of $P(2)$ only coverings by maximal subloops need be considered. Recall that the maximal subloops of $P(2)$ are of type $M_{24}(A_4, 2)$ and $M_{12}(S_3, 2)$.

Lemma 3.1 *The covering number of $P(2)$ is at least seven. Moreover, if $P(2)$ can be covered by seven maximal subloops then the intersection of any two of them would have an order that is not divisible by three.*

Proof From [7], along with the fact that $|P(2)| = 120$, there exist Sylow 3-subloops of $P(2)$ all of which are of order three. Thus, a lower bound for the covering number of $P(2)$ can be found by counting the number of Sylow 3-subloops of $P(2)$ and using the fact that any two distinct Sylow 3-subloops of $P(2)$ intersect trivially. We know from [8, Proposition 3.6] that if p is an odd prime that divides $q + 1$ then

$|\text{Syl}_p(P(q))| = (q^4 + q^3 + q^2)|\text{Syl}_p(\text{SL}_2(q))|$. Therefore, $|\text{Syl}_3(P(2))| = 28$. Since $|\text{Syl}_3(M_{12}(S_3, 2))| = |\text{Syl}_3(S_3)| = 1$ and $|\text{Syl}_3(M_{24}(A_4, 2))| = |\text{Syl}_3(A_4)| = 4$, one would have to use at least seven maximal subloops of the form $M_{24}(A_4, 2)$ to cover $P(2)$. Furthermore, since the Sylow 3-subloops of $P(2)$ intersect trivially, if $P(2)$ can be covered by seven maximal subloops of order 24 then the intersection of any two of them would have an order that is not divisible by three. \square

Theorem 3.2 *If $h_1 \in H$ and the six hexagon lines adjacent to h_1 are $h_2, \dots, h_7 \in H$ then $P(2) = \bigcup_{i=1}^7 \text{Stab}_C(h_i)^*$.*

Proof Since $G_2(2)$ is transitive on H , without loss of generality, we may assume that

$$h_1 = \left\{ \left(\begin{array}{cc} 0 & (x, 0, 0) \\ (0, y, 0) & 0 \end{array} \right) \middle| x, y \in F_2 \right\}.$$

Thus, the six hexagon lines adjacent to h_1 are:

$$\begin{aligned} h_2 &= \left\{ \left(\begin{array}{cc} 0 & (x, 0, 0) \\ (0, 0, y) & 0 \end{array} \right) \middle| x, y \in F_2 \right\}, \\ h_3 &= \left\{ \left(\begin{array}{cc} 0 & (x, 0, 0) \\ (0, y, y) & 0 \end{array} \right) \middle| x, y \in F_2 \right\}, \\ h_4 &= \left\{ \left(\begin{array}{cc} 0 & (0, 0, x) \\ (0, y, 0) & 0 \end{array} \right) \middle| x, y \in F_2 \right\}, \\ h_5 &= \left\{ \left(\begin{array}{cc} 0 & (x, 0, x) \\ (0, y, 0) & 0 \end{array} \right) \middle| x, y \in F_2 \right\}, \\ h_6 &= \left\{ \left(\begin{array}{cc} y & (x, 0, y) \\ (0, x, y) & y \end{array} \right) \middle| x, y \in F_2 \right\}, \quad \text{and} \\ h_7 &= \left\{ \left(\begin{array}{cc} y & (x + y, 0, y) \\ (0, x, y) & y \end{array} \right) \middle| x, y \in F_2 \right\}. \end{aligned}$$

Here

$$\begin{aligned} \text{Stab}_C(h_1) &= \left\{ \left(\begin{array}{cc} a & (b, 0, c) \\ (0, d, f) & g \end{array} \right) \middle| a, b, c, d, f, g \in F_2 \right\}, \\ \text{Stab}_C(h_2) &= \left\{ \left(\begin{array}{cc} a & (b, c, 0) \\ (0, d, f) & g \end{array} \right) \middle| a, b, c, d, f, g \in F_2 \right\}, \\ \text{Stab}_C(h_3) &= \left\{ \left(\begin{array}{cc} a & (b, c, c) \\ (0, d, f) & g \end{array} \right) \middle| a, b, c, d, f, g \in F_2 \right\}, \\ \text{Stab}_C(h_4) &= \left\{ \left(\begin{array}{cc} a & (b, 0, c) \\ (d, f, 0) & g \end{array} \right) \middle| a, b, c, d, f, g \in F_2 \right\}, \\ \text{Stab}_C(h_5) &= \left\{ \left(\begin{array}{cc} a & (b, 0, c) \\ (d, f, d) & g \end{array} \right) \middle| a, b, c, d, f, g \in F_2 \right\}, \end{aligned}$$

$$\text{Stab}_C(h_6) = \left\{ \begin{pmatrix} a & (b, c, d + a) \\ (c, f, d + g) & g \end{pmatrix} \middle| a, b, c, d, f, g \in F_2 \right\}, \quad \text{and}$$

$$\text{Stab}_C(h_7) = \left\{ \begin{pmatrix} a & (b, c, d + a) \\ (c, f, d + g + c) & g \end{pmatrix} \middle| a, b, c, d, f, g \in F_2 \right\}.$$

One should note that h_1, h_2 , and h_3 meet at the vertex $\langle \begin{pmatrix} 0 & (1,0,0) \\ (0,0,0) & 0 \end{pmatrix} \rangle$ and

$$\begin{aligned} \text{Stab}_C(h_1)^* \cap \text{Stab}_C(h_2)^* &= \text{Stab}_C(h_2)^* \cap \text{Stab}_C(h_3)^* \\ &= \text{Stab}_C(h_1)^* \cap \text{Stab}_C(h_3)^* \\ &= \left\{ \begin{pmatrix} 1 & (a, 0, 0) \\ (0, b, c) & 1 \end{pmatrix} \middle| a, b, c \in F_2 \right\} \\ &= I + \text{span}(h_1, h_2). \end{aligned}$$

Similarly, h_1, h_4 , and h_5 meet at the vertex $\langle \begin{pmatrix} 0 & (0,0,0) \\ (0,1,0) & 0 \end{pmatrix} \rangle$ and the hexagon lines h_1, h_6 , and h_7 meet at the vertex $\langle \begin{pmatrix} 0 & (1,0,0) \\ (0,1,0) & 0 \end{pmatrix} \rangle$ with

$$\begin{aligned} \text{Stab}_C(h_1)^* \cap \text{Stab}_C(h_4)^* &= \text{Stab}_C(h_4)^* \cap \text{Stab}_C(h_5)^* \\ &= \text{Stab}_C(h_1)^* \cap \text{Stab}_C(h_5)^* \\ &= \left\{ \begin{pmatrix} 1 & (a, 0, b) \\ (0, c, 0) & 1 \end{pmatrix} \middle| a, b, c \in F_2 \right\} \\ &= I + \text{span}(h_1, h_4) \end{aligned}$$

and

$$\begin{aligned} \text{Stab}_C(h_1)^* \cap \text{Stab}_C(h_6)^* &= \text{Stab}_C(h_6)^* \cap \text{Stab}_C(h_7)^* \\ &= \text{Stab}_C(h_1)^* \cap \text{Stab}_C(h_7)^* \\ &= \left\{ \begin{pmatrix} 1 + b & (a, 0, b) \\ (0, c, b) & 1 + b \end{pmatrix} \middle| a, b, c \in F_2 \right\} \\ &= I + \text{span}(h_1, h_6). \end{aligned}$$

Moreover, if $h_i, h_j \in \{h_2, \dots, h_7\}$ with $d(h_i, h_j) = 2$ then

$$\begin{aligned} \text{Stab}_C(h_i)^* \cap \text{Stab}_C(h_j)^* &= \left\{ \begin{pmatrix} 1 & (a, 0, 0) \\ (0, b, 0) & 1 \end{pmatrix} \middle| a, b \in F_2 \right\} \\ &= I + h_1. \end{aligned}$$

So if T is a nonempty subset of $\{h_1, \dots, h_7\}$ then

$$\left| \bigcap_{h_i \in T} \text{Stab}_C(h_i)^* \right| = \begin{cases} 24 & \text{if } |T| = 1, \\ 8 & \text{if } |T| > 1 \text{ and all of the lines} \\ & \text{in } T \text{ meet at a vertex,} \\ 4 = |I + h_1| & \text{if there exist } h_j, h_k \in T \text{ with} \\ & d(h_j, h_k) = 2. \end{cases}$$

Hence,

$$\begin{aligned} \left| \bigcup_{i=1}^7 \text{Stab}_C(h_i)^* \right| &= 7 \cdot 24 - (9 \cdot 8 + 24 \cdot 4) + (3 \cdot 8 + 32 \cdot 4) \\ &\quad - \binom{7}{4} \cdot 4 + \binom{7}{5} \cdot 4 - \binom{7}{6} \cdot 4 + \binom{7}{7} \cdot 4 \\ &= 120 \\ &= |P(2)| \end{aligned}$$

and $P(2) = \bigcup_{i=1}^7 \text{Stab}_C(h_i)^*$. □

From Theorem 3.2 along with Lemma 3.1, we get that the covering number of $P(2)$ is seven. Furthermore, $P(2) = \bigcup_{i=1}^7 \text{Stab}_C(h_i)^*$ for any set of hexagon lines $h_1, \dots, h_7 \in H$ where $d(h_1, h_i) = 1$ for all $2 \leq i \leq 7$.

4 Uniqueness of a covering with seven subloops

We are now ready to show that $G_2(2)$ permutes the coverings of $P(2)$ with seven subloops transitively.

Lemma 4.1 *If $h_1, h_2 \in H$ with $d(h_1, h_2) = 3$ then $\text{Stab}_C(h_1)^* \cap \text{Stab}_C(h_2)^* \cong S_3$ and is of order six.*

Proof From [1, Sect. 17], the group $G_2(2)$ is distance-transitive on the generalized hexagon. So without loss of generality, we may assume that

$$\begin{aligned} h_1 &= \left\{ \begin{pmatrix} 0 & (x, 0, 0) \\ (0, y, 0) & 0 \end{pmatrix} \middle| x, y \in F_2 \right\} \\ \text{and } h_2 &= \left\{ \begin{pmatrix} 0 & (0, x, 0) \\ (y, 0, 0) & 0 \end{pmatrix} \middle| x, y \in F_2 \right\}. \end{aligned}$$

Since

$$\text{Stab}_C(h_1) = \left\{ \begin{pmatrix} a & (b, 0, c) \\ (0, d, f) & g \end{pmatrix} \middle| a, b, c, d, f, g \in F_2 \right\}$$

$$\text{and } \text{Stab}_C(h_2) = \left\{ \begin{pmatrix} a & (0, b, c) \\ (d, 0, f) & g \end{pmatrix} \middle| a, b, c, d, f, g \in F_2 \right\},$$

$$\text{Stab}_C(h_1)^* \cap \text{Stab}_C(h_2)^* = \left\{ \begin{pmatrix} a & (0, 0, b) \\ (0, 0, c) & d \end{pmatrix} \middle| a, b, c, d \in F_2 \right\}^*$$

$$\cong S_3. \quad \square$$

Now suppose $h_1, \dots, h_7 \in H$ satisfy $P(2) = \bigcup_{i=1}^7 \text{Stab}_C(h_i)^*$. Since three divides the order of S_3 , by Lemmas 3.1 and 4.1, $d(h_i, h_j) \leq 2$ for all $i, j \in \{1, 2, \dots, 7\}$.

Theorem 4.2 *If $h_1, \dots, h_7 \in H$ satisfy $P(2) = \bigcup_{i=1}^7 \text{Stab}_C(h_i)^*$ then there exists an $i \in \{1, \dots, 7\}$ such that $d(h_i, h_j) \leq 1$ for all $j \in \{1, \dots, 7\}$.*

Proof First assume that $d(h_i, h_j) = 2$ for all $i, j \in \{1, \dots, 7\}$ with $i \neq j$. Clearly, for any pair of lines h_i and h_j there exists at most one line h_k with $k \in \{1, \dots, 7\} \setminus \{1, 2\}$ such that h_i, h_j , and h_k are all adjacent to some line M . Thus at least four of these lines are contained in a hexagon with h_i and h_j . Without loss of generality, let $i = 1, j = 2$, and h_3, h_4, h_5, h_6 be contained in a hexagon with h_1 and h_2 . Then at least two of h_4, h_5, h_6 are contained in a hexagon with h_1 and h_3 , say h_4, h_5 . Similarly, at least one of these is contained in a hexagon with h_2 and h_3 , say h_4 . Hence, any three of the lines h_1, h_2, h_3, h_4 are contained in a hexagon. But this contradicts the main result of [9].

Now suppose that $d(h_1, h_2) = 1$. Let p be the vertex incident to both h_1 and h_2 and let M be the third line containing p . If $d(h_i, h_3) = 2$ for $i \in \{1, 2\}$ then clearly $d(h_3, M) = 1$. In this case, none of h_4, h_5, h_6, h_7 are at distance one from either h_1 or h_2 except for M . Hence, without loss of generality, we may assume that $h_4 = M$ and that h_5, h_6 , and h_7 are at distance one from h_4 . Now if $d(h_1, h_3) = 1$ and $h_3 \neq M$ then all of the lines h_4, h_5, h_6 , and h_7 are at distance one from h_1 . Hence, since $G_2(2)$ is transitive on H , there exists a unique line h_i such that $d(h_i, h_j) \leq 1$ for all $j \in \{1, \dots, 7\}$. □

With $G_2(2)$ being transitive on H , it immediately follows from Theorem 4.2 that $G_2(2)$ permutes the coverings of $P(2)$ with seven subloops transitively.

Problem Knowing that there does indeed exist Moufang loops that have a covering number of seven, the next question that arises is:
Does there exist a Moufang loop whose covering number is eleven?

References

1. Buekenhout, F., Cohen, A.M.: Diagram Geometry. Springer, New York (to appear)
2. Chein, O.: Moufang loops of small order I. Trans. Am. Math. Soc. **188**, 31–51 (1974)
3. Cohen, A.M., Tits, J.: On generalized hexagons and a near octagon whose lines have three points. Eur. J. Comb. **6**, 13–27 (1985)

4. Detomi, E., Lucchini, A.: On the structure of primitive n -sum groups. *CUBA Math. J.* **10**, 195–210 (2008)
5. Foguel, T., Kappe, L.C.: On loops covered by subloops. *Expo. Math.* **23**, 255–270 (2005)
6. Gagola, S.M. III: Subloops of the unit octonions. *Acta Sci. Math.* **72**, 837–861 (2006)
7. Gagola, S.M. III: The development of Sylow p -subloops in finite Moufang loops. *J. Algebra* **322**(5), 1565–1574 (2009)
8. Gagola, S.M. III: The number of Sylow p -subloops in finite Moufang loops. *Commun. Algebra* **38**(4), 1436–1448 (2010)
9. Kantor, W.M.: Generalized quadrangles associated with $G_2(q)$. *J. Comb. Theory, Ser. A* **29**, 212–219 (1980)
10. Liebeck, M.W.: The classification of finite simple Moufang loops. *Math. Proc. Camb. Philos. Soc.* **102**, 33–47 (1987)
11. Schellekens, G.L.: On a hexagonic structure. I, II. *Proc. K. Ned. Akad. Wet.* **65**, 201–234 (1962)
12. Tits, J.: Sur la trialité et certains groupes qui s'en déduisent. *Inst. Hautes Études Sci. Publ. Math.* **2**, 13–60 (1959)
13. Tomkinson, M.J.: Groups as the union of proper subgroups. *Math. Scand.* **81**, 189–198 (1997)