Norbert Hungerbühler* and Gideon Villiger

Exotic Steiner chains in Miquelian Möbius planes of odd order

DOI 10.1515/advgeom-2020-0035. Received 13 November, 2018; revised 22 June, 2019

Abstract: In the Euclidean plane, two circles that intersect or are tangent clearly do not carry a finite Steiner chain of circles. We show that such exotic Steiner chains exist in finite Miquelian Möbius planes of odd order. We obtain explicit conditions in terms of the order of the plane and the capacitance of the two carrier circles for the existence, length, and number of Steiner chains.

Keywords: Finite Möbius planes, Steiner's Theorem, Steiner chains, capacitance.

2010 Mathematics Subject Classification: 05B25, 51E30, 51B10

Communicated by: G. Korchmáros

1 Introduction

When Jakob Steiner was still a pupil in Yverdon's Pestalozzi school, he found his famous theorem in circle geometry (from his notes during his first month in Yverdon: "Found on Saturday Dec. 10th, 1814, after $3+3+4$ hours of efforts, at 1 o'clock in the night"):

Theorem (Steiner's porism). *Let C_1, C_2 be two disjoint Möbius circles (circles or straight lines) in the Euclidean plane. Consider a sequence of different Möbius circles $M_1, M_2, \dots, M_k$ which are tangent to both C_1 and C_2, and let M_i and M_{i+1} be tangent for $i = 1, \dots, k-1$. Then the following is true: If M_1 and M_k are tangent, then there are infinitely many such chains: Every point of C_1 and C_2 belongs to a circle of such a chain. And every chain of consecutive tangent circles closes after exactly k steps.*

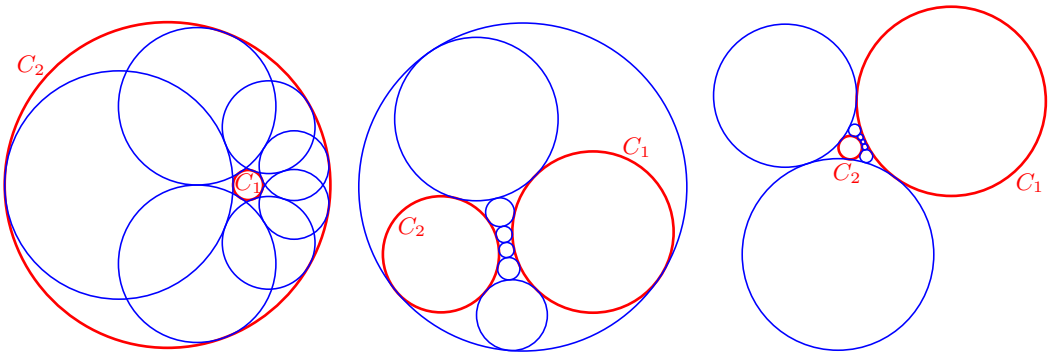

Figure 1: Left: Steiner chain wrapping around twice. Middle and right: carrier circles which are not nested.

Later Steiner investigated the geometric properties of such chains. For example, he proved that the tangent points of the circles $M_1, \dots, M_k$ lie on a circle and that their centers lie on a conic whose foci are the centers of the carrier circles C_1 and C_2. He also stated conditions for such a chain to close after k steps in terms of

***Corresponding author: Norbert Hungerbühler,** Department of Mathematics, ETH Zürich, Switzerland, email: norbert.hungerbuehler@math.ethz.ch
Gideon Villiger, Institute of Mathematics, University of Zürich, Switzerland, email: gideon.villiger@kswo.ch

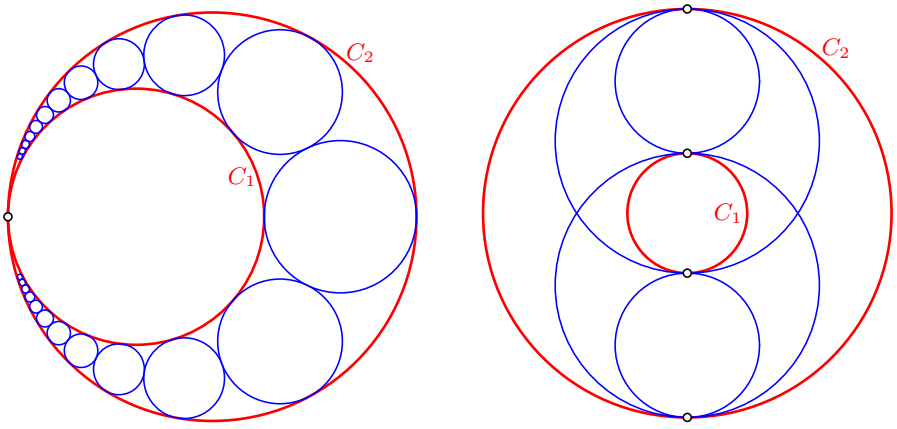

Figure 2: Pappus chain (left), degenerate Steiner chain (right)

the radii and the distance between the centers of C_1 and C_2. The interested reader will find more information about the classical theory of Steiner chains and generalizations in [2], [7], [3], [9], or [1].

Throughout this paper, p denotes an odd prime number, $m \geq 1$ a natural number, and $q = p^m$. It is known that a version of Steiner's porism holds in a finite Miquelian Möbius plane $\mathbb{M}(q)$. However, unlike in the Euclidean plane, a pair of circles in such a finite plane may or may not have a common tangent circle. If we fix a pair C_1, C_2 of disjoint circles and choose a point P on one of them, then the following is true: if $q \equiv -1 \bmod 4$ and the given pair C_1, C_2 admits a common tangent circle, then the pair carries precisely one Steiner chain such that P is a point of one of its circles. If $q \equiv 1 \bmod 4$ and if the pair C_1, C_2 admits a common tangent circle, then there exists either no Steiner chain, or precisely two of them, each with a circle containing P. The full statement is the following theorem (see Section 2 for definitions):

Theorem (Theorem 5.5 in [5]). *Let C_1 and C_2 be disjoint circles in the Miquelian Möbius plane $\mathbb{M}(q)$, $c := \operatorname{cap}(C_1, C_2)$ their capacitance, and P an arbitrary point on C_1 or C_2. Then $b := \frac{1}{2}(c-2+\sqrt{c(c-4)}) \in \mathrm{GF}(q)\setminus\{0\}$. If b is a nonsquare in $\mathrm{GF}(q)$, then C_1 and C_2 have no common tangent circles and hence they do not carry a Steiner chain. If, on the other hand, $b = \mu^2$, for $\mu = \mu_1$ and $\mu = \mu_2 = -\mu_1 \neq \mu_1 \in \mathrm{GF}(q)$, then for each $j \in \{1, 2\}$ satisfying the following conditions there is a separate Steiner chain of length $k \geq 3$ carried by C_1 and C_2 such that P belongs to one of its circles:*

(1) *$-\mu_j$ is a nonsquare in $\mathrm{GF}(q)$,*

(2) *$\xi := (-\mu_j^2 + 6\mu_j - 1 + 4(\mu_j - 1)\sqrt{-\mu_j})(1+\mu_j)^{-2}$ is a root of unity of order k, i.e. $\xi^k = 1 \neq \xi^l$ for $1 \leq l \leq k-1$.*

In the Euclidean plane, finite Steiner chains do not exist if C_1 and C_2 intersect or are tangent; the latter case corresponds to a Pappus chain (see Figure 2). A finite Möbius plane has only finitely many circles, thus it is conceivable that a Pappus chain closes after finitely many steps. We investigate the questions whether Steiner chains exist if the carrier circles intersect or are tangent to each other. The easier case, when the carrier circles are tangent, is treated in Section 3. The more delicate case of intersecting carrier circles is discussed in Section 4. Since these chains do not exist in the classical Möbius plane, we call them *exotic Steiner chains*.

2 Preliminaries

A Möbius plane is a triple $(\mathbb{P}, \mathbb{B}, \mathbb{I})$ of points $\mathbb{P}$, circles $\mathbb{B}$ and an incidence relation $\mathbb{I}$, satisfying three axioms:

(M1) For any three elements $P, Q, R \in \mathbb{P}$, $P \neq Q$, $P \neq R$ and $Q \neq R$, there exists a unique element $C \in \mathbb{B}$ with $P \in C$, $Q \in C$ and $R \in C$.

(M2) For any $C \in \mathbb{B}$, $P, Q \in \mathbb{P}$ with $P \in C$ and $Q \notin C$, there exists a unique element $D \in \mathbb{B}$ such that $P \in D$ and $Q \in D$, but for all $R \in \mathbb{P}$ with $R \in C$, $P \neq R$, we have $R \notin D$.

(M3) There are four elements $P_1, P_2, P_3, P_4 \in \mathbb{P}$ such that for all $C \in \mathbb{B}$, we have $P_i \notin C$ for at least one $i \in \{1, 2, 3, 4\}$. Moreover, for all $C \in \mathbb{B}$ there exists a $P \in \mathbb{P}$ with $P \in C$.

A Steiner chain in a Möbius plane is defined as follows:

Definition 1. Given two circles C_1, C_2, we say that they carry a (proper) *Steiner chain of length* $k \geq 3$, if there exists a sequence (chain) of distinct circles $M_1, \ldots, M_k$ such that

(i) each circle M_i is tangent to the next one M_{i+1}, where indices are taken cyclically,

(ii) each circle in the chain is tangent to C_1 and C_2, and

(iii) no point is contact point of more than two tangent circles.

Condition (iii) excludes degenerate Steiner chains as the one in Figure 2.

To fix notation and to make this presentation selfcontained, we briefly describe the construction of a finite Miquel plane over the Galois field $\mathrm{GF}(q)$ and its quadratic extension $\mathrm{GF}(q)(\alpha) \cong \mathrm{GF}(q^2)$, where α is a nonsquare in $\mathrm{GF}(q)$. The conjugation $\mathrm{GF}(q^2) \to \mathrm{GF}(q^2) : z \mapsto \overline{z} := z^q$ is an automorphism of $\mathrm{GF}(q^2)$, whose fixed point set is $\mathrm{GF}(q)$; see e.g. [6, Theorem 2.21]. The *norm* and the *trace* are defined by

$$\mathrm{N} : \mathrm{GF}(q^2) \to \mathrm{GF}(q) : z \mapsto z\overline{z} \qquad \text{and} \qquad \mathrm{Tr} : \mathrm{GF}(q^2) \to \mathrm{GF}(q) : z \mapsto z + \overline{z}.$$

The finite Miquelian Möbius plane constructed over the pair $\mathrm{GF}(q)$ and $\mathrm{GF}(q^2)$ is denoted by $\mathbb{M}(q)$, and q is called the *order* of $\mathbb{M}(q)$: The q^2+1 points of $\mathbb{M}(q)$ are the elements of $\mathrm{GF}(q^2)$ together with a point at infinity, denoted by ∞. There are two different types of circles: Circles of the first type are solutions of the equation $\mathrm{N}(z-c) = r$, i.e.

$$B^1_{(c,r)} : (z-c)(\overline{z}-\overline{c}) = r \tag{1}$$

for $c \in \mathrm{GF}(q^2)$ and $r \in \mathrm{GF}(q)\backslash\{0\}$. There are $q+1$ points in $\mathrm{GF}(q^2)$ on every such circle, and there are $q^2(q-1)$ circles of the first type. Circles of the second type are solutions of the equation $\mathrm{Tr}(\overline{c}z) = r$, i.e.

$$B^2_{(c,r)} : \overline{c}z + c\overline{z} = r \tag{2}$$

for $c \in \mathrm{GF}(q^2)\backslash\{0\}$ and $r \in \mathrm{GF}(q)$, together with ∞. Hence, there are $q(q+1)$ circles of the second type, each containing also $q+1$ points.

Let $a, b, c, d \in \mathrm{GF}(q^2)$ such that $ad - bc \neq 0$. The bijective map $\Phi : \mathbb{M}(q) \to \mathbb{M}(q)$ defined by

$$\Phi(z) = \frac{az+b}{cz+d} \quad \text{if } z \neq \infty \text{ and } cz+d \neq 0,$$

$\Phi(z) = \infty$ if $z \neq \infty$ and $cz + d = 0$, $\Phi(\infty) = ac^{-1}$ if $c \neq 0$ and $\Phi(\infty) = \infty$ if $c = 0$ is called a *Möbius transformation* of $\mathbb{M}(q)$. Every Möbius transformation is an automorphism of $\mathbb{M}(q)$: It maps circles to circles and preserves incidence. The Möbius transformations operate sharply triply transitive, i.e. there is a unique Möbius transformation mapping any three points into any other three points. For more information on finite Möbius planes see [4].

The following lemma, which is proved by an elementary computation, gives the conditions for the mutual position of two circles.

Lemma 2. (i) *Let $B^1_{(c_1,r_1)}$ and $B^1_{(c_2,r_2)}$ be two distinct circles of the first type, and $D := (c\overline{c} + r_1 - r_2)^2 - 4c\overline{c}r_1$ for $c = c_2 - c_1$. Then:*

- *If $D \neq 0$ is a square in $\mathrm{GF}(q)$, the circles are disjoint.*
- *If $D = 0$, the circles touch at $z_0 = \frac{c\overline{c}+r_1-r_2}{2\overline{c}} + c_1 = \frac{1}{2}\big(c_2 + c_1 - \frac{r_2-r_1}{\overline{c}_2-\overline{c}_1}\big)$.*
- *If D is a nonsquare in $\mathrm{GF}(q)$, the circles intersect at $z_{1,2} = \frac{(c\overline{c}+r_1-r_2)\pm\sqrt{D}}{2\overline{c}} + c_1$.*

(ii) *Let $B^1_{(c_1,r_1)}$ and $B^2_{(c_2,r_2)}$ be a circle of the first type and of the second type, respectively, and let $D := r^2 - 4c_2\overline{c}_2r_1$ for $r = r_2 - c_1\overline{c}_2 - \overline{c}_1c_2$. Then:*

- *If $D \neq 0$ is a square in $\mathrm{GF}(q)$, the circles are disjoint.*
- *If $D = 0$, the circles touch at $z_0 = \frac{r}{2\overline{c}_2} + c_1 = \frac{r_2+c_1\overline{c}_2-\overline{c}_1c_2}{2\overline{c}_2}$.*
- *If D is a nonsquare in $\mathrm{GF}(q)$, the circles intersect at $z_{1,2} = \frac{r\pm\sqrt{D}}{2\overline{c}_2} + c_1$.*

(iii) *Let $B^2_{(c_1,r_1)}$ and $B^2_{(c_2,r_2)}$ be two distinct circles of the second type. Then:*
- *If $c_1\overline{c}_2 - \overline{c}_1 c_2 = 0$, the circles touch at ∞.*
- *If $c_1\overline{c}_2 - \overline{c}_1 c_2 \neq 0$, the circles intersect at ∞ and $z_0 = \frac{c_1 r_2 - c_2 r_1}{c_1\overline{c}_2 - \overline{c}_1 c_2}$.*

Below we use Möbius transformations to bring two general carrier circles to a standard position. In order to formulate conditions on the existence of Steiner chains for intersecting carrier circles in an arbitrary position we need the capacitance, which was introduced in [5]:

Definition 3. The *capacitance* assigns an element of $\mathrm{GF}(q)$ to any pair of circles in $\mathbb{M}(q)$. It is defined as

$$\operatorname{cap}(B^1_{(c_1,r_1)}, B^1_{(c_2,r_2)}) := \frac{1}{r_1 r_2}\big(r_1 + r_2 - (c_1 - c_2)(\overline{c}_1 - \overline{c}_2)\big)^2,$$
$$\operatorname{cap}(B^1_{(c_1,r_1)}, B^2_{(c_2,r_2)}) := \operatorname{cap}(B^2_{(c_2,r_2)}, B^1_{(c_1,r_1)}) := \frac{1}{r_1 c_2\overline{c}_2}(c_1\overline{c}_2 + \overline{c}_1 c_2 - r_2)^2, \quad \text{and}$$
$$\operatorname{cap}(B^2_{(c_1,r_1)}, B^2_{(c_2,r_2)}) := \frac{1}{c_1\overline{c}_1 c_2\overline{c}_2}(c_1\overline{c}_2 + \overline{c}_1 c_2)^2.$$

The remarkable property of the capacitance is its invariance under Möbius transformations:

Theorem 4 (Theorem 5.1 in [5]). *If $B, B' \in \mathbb{M}(q)$ are circles and Φ is a Möbius transformation, then* $\operatorname{cap}(B, B') = \operatorname{cap}(\Phi(B), \Phi(B'))$.

3 Exotic Steiner chains in tangent carrier circles

3.1 The standard case

Let us start with the two circles $B_{-1} := B^2_{(1,-1)}$ and $B_1 := B^2_{(1,1)}$ in $\mathbb{M}(q)$ with equations

$$B_{-1}\colon z + \overline{z} = -1 \quad \text{and} \quad B_1\colon z + \overline{z} = 1.$$

These circles of the second type are different as p is odd, and since both equations cannot be satisfied at the same time, the circles are tangent at ∞. Let $\tau(B_{-1}, B_1)$ be the set of all common tangent circles of B_{-1} and B_1 of the first type. Observe that circles of the second type cannot belong to a proper Steiner chain carried by B_{-1} and B_1, because ∞ is already used as the contact point of the carrier circles B_{-1} and B_1 (see Definition 1(iii)).

According to Lemma 2, $B^1_{(c,r)}$ is in $\tau(B_{-1}, B_1)$ if and only if $(c + \overline{c} + 1)^2 = 4r$ and $(c + \overline{c} - 1)^2 = 4r$. This implies $c + \overline{c} = 0$ and $4r = 1$. The condition for c is the equation of a circle of the second type, so there are q circles of the first type in $\tau(B_{-1}, B_1)$. Hence we have the following:

Lemma 5. *There are q circles of the first type tangent to both B_{-1} and B_1. They are given by $B^1_{(c,r)}$ with $c \in B_0 := B^2_{(1,0)}$ and $r = \frac{1}{4}$.*

As we are trying to construct a chain of circles, we pick $B^1_{(0,\frac{1}{4})} \in \tau(B_{-1}, B_1)$ as our starting circle. Lemma 6 tells us under what circumstances such a chain may possibly exist.

Lemma 6. *If -1 is a nonsquare in $\mathrm{GF}(q)$, then there are exactly two circles $B^1_{(c,r)} \in \tau(B_{-1}, B_1)$ tangent to $B^1_{(0,\frac{1}{4})}$. They are given by $c = \pm\sqrt{-1}$ and $r = \frac{1}{4}$. If -1 is a square in $\mathrm{GF}(q)$, then there are no common tangent circles of B_{-1}, B_1 and $B^1_{(0,\frac{1}{4})}$.*

Proof. Let $B^1_{(c,r)}$ be in $\tau(B_{-1}, B_1)$, i.e. $c + \overline{c} = 0$ and $r = \frac{1}{4}$. For $B^1_{(c,r)}$ to be tangent to $B^1_{(0,\frac{1}{4})}$ as well, it has to satisfy the condition from Lemma 2(i), i.e. $c^2(c^2 + 1) = 0$ since $\overline{c} = -c$. As $c \neq 0$ (otherwise $B^1_{(c,r)}$ coincides with $B^1_{(0,\frac{1}{4})}$), it follows that $c^2 = -1$ and thus $c = \pm\sqrt{-1}$. Moreover, the relation $\overline{c} = -c$ makes it clear that $c \notin \mathrm{GF}(q)$. Consequently, there only exists a solution if -1 is a nonsquare in $\mathrm{GF}(q)$. □

Assume now that -1 is a nonsquare in $\mathrm{GF}(q)$. As we have seen, in this case the two circles $B^1_{(0,\frac{1}{4})}$ and $B^1_{(\sqrt{-1},\frac{1}{4})}$ are in $\tau(B_{-1}, B_1)$ and are tangent. We apply the Möbius transformation $T : z \mapsto z + \sqrt{-1}$: Indeed,

T leaves B_{-1} and B_1 invariant, $B^1_{(0,\frac{1}{4})}$ is mapped to $B^1_{(\sqrt{-1},\frac{1}{4})}$, while $B^1_{(\sqrt{-1},\frac{1}{4})}$ is mapped to $B^1_{(2\sqrt{-1},\frac{1}{4})}$. By the properties of Möbius transformations, both circles are still tangent to each other, as well as tangent to B_{-1} and B_1. This induces a Steiner chain: By applying the above translation k times, we get the k-th circle in the chain, and for $k = p$ we are back to our starting circle:

$$B^1_{(0,\frac{1}{4})} \to B^1_{(\sqrt{-1},\frac{1}{4})} \to B^1_{(2\sqrt{-1},\frac{1}{4})} \to \cdots \to B^1_{(p\sqrt{-1},\frac{1}{4})} = B^1_{(0,\frac{1}{4})}.$$

Recall that there are $q = p^m$ circles in $\tau(B_{-1}, B_1)$. Hence there are exactly p^{m-1} Steiner chains of length p each. Therefore we have:

Proposition 7. *The circles $B^2_{(1,-1)}$ and $B^2_{(1,1)}$ in $\mathbb{M}(q)$, $q = p^m$, carry a Steiner chain if and only if $q \equiv 3 \bmod 4$. In this case there are p^{m-1} different Steiner chains, and each chain has length p.*

3.2 The general case

Let C_1 and C_2 be two circles in $\mathbb{M}(q)$ that are tangent at z_0. Choose two points z_1, z_2 on C_1 and two points z_1', z_2' on B_{-1}. There is a Möbius transformation T_1 which maps z_i to z_i' and z_0 to ∞, hence $T_1(C_1) = B_{-1}$ and $T_1(C_2)$ is a circle of the second kind tangent to B_{-1} at ∞. By Lemma 2, for any circle $B^2_{(c,r)}$ tangent to B_{-1} we have $c \in \mathrm{GF}(q)$, thus $T_1(C_2)$ has the form $z+\overline{z} = r$ for $r \neq -1$. The Möbius transformation $T_2 : z \mapsto \lambda(z+\frac{1}{2})-\frac{1}{2}$, with $\lambda = \frac{2}{r+1}$, maps B_{-1} to itself, and $T_1(C_2)$ to B_1. Hence $T = T_2 \circ T_1$ maps C_1 to B_{-1} and C_2 to B_1, and an exotic Steiner chain exists for C_1, C_2 if and only if this is the case for B_{-1}, B_1. Hence we have:

Theorem 8. *Let C_1 and C_2 be two tangent circles in $\mathbb{M}(q)$, $q = p^m$. If $q \equiv 3 \bmod 4$, then C_1 and C_2 carry p^{m-1} Steiner chains, and each chain has length p. If $q \equiv 1 \bmod 4$, then C_1 and C_2 do not carry a Steiner chain.*

4 Exotic Steiner chains for intersecting carrier circles

The case of intersecting carrier circles is particularly more delicate than the case of tangent carrier circles treated in the previous section. We start again by a standard situation.

4.1 The standard case

We start with two different circles of the second type $B^2_{(\gamma_1,0)}$ and $B^2_{(\gamma_2,0)}$ intersecting in 0 and ∞. By Lemma 2 we have $\gamma_1\overline{\gamma}_2 - \overline{\gamma}_1\gamma_2 \neq 0$, which is needed in the proof of:

Lemma 9. *If $\gamma_1\gamma_2$ is a square in $\mathrm{GF}(q^2)$, there are exactly $2(q-1)$ circles in $\tau(B^2_{(\gamma_1,0)}, B^2_{(\gamma_2,0)})$. If $\gamma_1\gamma_2$ is a non-square, then $B^2_{(\gamma_1,0)}$ and $B^2_{(\gamma_2,0)}$ have no common tangent circles.*

Proof. We observe that there are no circles of the second type tangent to both $B^2_{(\gamma_1,0)}$ and $B^2_{(\gamma_2,0)}$: By Lemma 2, any such circle $B^2_{(c,r)}$ would satisfy $c\overline{\gamma}_1 - \overline{c}\gamma_1 = 0$ and $c\overline{\gamma}_2 - \overline{c}\gamma_2 = 0$, which implies $c(\gamma_1\overline{\gamma}_2 - \overline{\gamma}_1\gamma_2) = 0$. But $c \neq 0$ for a circle of the second type, and this contradicts $\gamma_1\overline{\gamma}_2 - \overline{\gamma}_1\gamma_2 \neq 0$.

For any circle $B^1_{(c,r)}$ of the first type in $\tau(B^2_{(\gamma_1,0)}, B^2_{(\gamma_2,0)})$ we have

$$(c\overline{\gamma}_1 + \overline{c}\gamma_1)^2 = 4\gamma_1\overline{\gamma}_1 r \tag{3}$$

and

$$(c\overline{\gamma}_2 + \overline{c}\gamma_2)^2 = 4\gamma_2\overline{\gamma}_2 r \tag{4}$$

as a consequence of Lemma 2. Note that $4\gamma_i\overline{\gamma}_i r \neq 0$ because of the way the circles are defined, and since p is odd. Eliminating $r = \frac{(c\overline{\gamma}_2+\overline{c}\gamma_2)^2}{4\gamma_2\overline{\gamma}_2}$ from (3) leads to

$$\gamma_2\overline{\gamma}_2(c^2\overline{\gamma}_1^2 + \overline{c}^2\gamma_1^2) = \gamma_1\overline{\gamma}_1(c^2\overline{\gamma}_2^2 + \overline{c}^2\gamma_2^2) \iff c^2\overline{\gamma}_1\overline{\gamma}_2 \cdot (\overline{\gamma}_1\gamma_2 - \gamma_1\overline{\gamma}_2) = \overline{c}^2\gamma_1\gamma_2(\overline{\gamma}_1\gamma_2 - \gamma_1\overline{\gamma}_2).$$

Since $\gamma_1\overline{\gamma}_2 - \overline{\gamma}_1\gamma_2 \neq 0$, this is equivalent to $c^2\overline{\gamma}_1\overline{\gamma}_2 = \overline{c}^2\gamma_1\gamma_2$. Thus any c satisfying (3) and (4) is characterized by the condition $c^2\overline{\gamma}_1\overline{\gamma}_2 =: \beta \in \mathrm{GF}(q) \setminus \{0\}$, i.e.

$$c^2 = \beta/(\overline{\gamma}_1\overline{\gamma}_2) \quad \text{for } \beta \in \mathrm{GF}(q) \setminus \{0\}.$$

This can be solved for c if and only if $\gamma_1\gamma_2$ is a square in $\mathrm{GF}(q^2)$, and in this case, c is given by

$$c = \pm\sqrt{\beta/(\overline{\gamma}_1\overline{\gamma}_2)}. \tag{5}$$

There are $q-1$ possible choices for $\beta \in \mathrm{GF}(q) \setminus \{0\}$, and thus $2(q-1)$ different values that $\pm\sqrt{\beta}$ can attain. Since there is a unique r corresponding to every c, there are exactly $2(q-1)$ circles in $\tau(B^2_{(\gamma_1,0)}, B^2_{(\gamma_2,0)})$. □

From now on we assume that $\gamma_1\gamma_2$ is a square in $\mathrm{GF}(q^2)$, i.e. $\tau(B^2_{(\gamma_1,0)}, B^2_{(\gamma_2,0)})$ is non-empty. Observe that $\gamma_1\gamma_2$ is a square if and only if both γ_1 and γ_2 are either squares or nonsquares. This also implies that $\gamma_1\gamma_2$ is a square if and only if $\frac{\overline{\gamma}_2}{\overline{\gamma}_1}$ is a square. So, we define $\gamma := \sqrt{\frac{\overline{\gamma}_2}{\overline{\gamma}_1}}$ to be a square root of $\frac{\overline{\gamma}_2}{\overline{\gamma}_1}$, and apply the Möbius transformation $z \mapsto \overline{\gamma}_1\gamma z$ to the carrier circles

$$B^2_{(\gamma_1,0)}\colon \overline{\gamma}_1 z + \gamma_1\overline{z} = 0 \quad \text{and} \quad B^2_{(\gamma_2,0)}\colon \overline{\gamma}_2 z + \gamma_2\overline{z} = 0.$$

The images of the circles $B^2_{(\gamma_1,0)}$ and $B^2_{(\gamma_2,0)}$ are then given by the equations $\overline{\gamma}z + \gamma\overline{z} = 0$ and $\gamma z + \overline{\gamma z} = 0$, respectively. We summarize what we have shown so far: If $\gamma_1\gamma_2$ is a nonsquare, no Steiner chain exists. But if $\gamma_1\gamma_2$ is a square, we can transform the circles $B^2_{(\gamma_1,0)}, B^2_{(\gamma_2,0)}$ into the two symmetric circles $B^2_{(\gamma,0)}$ and $B^2_{(\overline{\gamma},0)}$, where γ is defined as above. Note that the condition $\gamma_1\overline{\gamma}_2 - \overline{\gamma}_1\gamma_2 \neq 0$ changes to $\gamma^2 \neq \overline{\gamma}^2$.

We now state an explicit condition for a circle to be in $\tau(B^2_{(\gamma,0)}, B^2_{(\overline{\gamma},0)})$.

Lemma 10. *There are $2(q-1)$ circles tangent to $B^2_{(\gamma,0)}$ and $B^2_{(\overline{\gamma},0)}$ with $\gamma^2 \neq \overline{\gamma}^2$. They are given by $B^1_{(c,r)}$ with c and r satisfying*

$$c = \overline{c}, \qquad r = c^2\frac{(\gamma+\overline{\gamma})^2}{4\gamma\overline{\gamma}} \tag{6}$$

or

$$c = -\overline{c}, \qquad r = c^2\frac{(\gamma-\overline{\gamma})^2}{4\gamma\overline{\gamma}} \tag{7}$$

for $c \in \mathrm{GF}(q^2) \setminus \{0\}$.

Proof. By Lemma 2, the condition for a circle $B^1_{(c,r)}$ to be in $\tau(B^2_{(\gamma,0)}, B^2_{(\overline{\gamma},0)})$ is

$$(c\overline{\gamma} + \overline{c}\gamma)^2 = 4\gamma\overline{\gamma}r \quad \text{and} \quad (c\gamma + \overline{c\gamma})^2 = 4\gamma\overline{\gamma}r. \tag{8}$$

We subtract the second equation in (8) from the first and get $(c^2 - \overline{c}^2)(\overline{\gamma}^2 - \gamma^2) = 0$. Since $\gamma^2 \neq \overline{\gamma}^2$, this implies $c^2 - \overline{c}^2 = (c-\overline{c})(c+\overline{c}) = 0$. Plugging in the respective values $\overline{c} = c$ and $\overline{c} = -c$ in (8) yields the r-values specified in the lemma. We also see that c is nonzero, as $c = 0$ would lead to $r = 0$. □

We established in Lemma 10 that the center c_1 of any circle $B^1_{(c_1,r_1)}$ tangent to both carrier circles is either on the circle $z - \overline{z} = 0$ (i.e. $z \in \mathrm{GF}(q)$) or on the circle $z + \overline{z} = 0$. Accordingly, we subsequently investigate what the conditions are for a second circle $B^1_{(c_2,r_2)} \in \tau(B^2_{(\gamma,0)}, B^2_{(\overline{\gamma},0)})$ to be tangent to $B^2_{(c_1,r_1)}$ if

- both c_1 and c_2 are on $z - \overline{z} = 0$ (see Lemma 11),
- both c_1 and c_2 are on $z + \overline{z} = 0$ (see Lemma 12), and
- c_1 and c_2 are not on the same line (see Lemma 13).

Lemma 11. *Let $B^1_{(c_1,r_1)}, B^1_{(c_2,r_2)} \in \tau(B^2_{(\gamma,0)}, B^2_{(\overline{\gamma},0)})$ with $c_1 = \overline{c}_1$ and $c_2 = \overline{c}_2$. The circles $B^1_{(c_1,r_1)}$ and $B^1_{(c_2,r_2)}$ are tangent if and only if $\gamma\overline{\gamma}$ is a square in $\mathrm{GF}(q)$ and*

$$c_2 = c_1 \cdot \frac{2\sqrt{\gamma\overline{\gamma}} \pm (\gamma+\overline{\gamma})}{2\sqrt{\gamma\overline{\gamma}} \mp (\gamma+\overline{\gamma})}. \tag{9}$$

Proof. Recall that both circles $B^1_{(c_1,r_1)}$ and $B^1_{(c_2,r_2)}$ satisfy equation (6) from Lemma 10, namely:

$$c_i = \overline{c}_i, \quad r_i = c_i^2 \frac{(\gamma+\overline{\gamma})^2}{4\gamma\overline{\gamma}}, \qquad c_i \neq 0, \quad i = 1, 2. \tag{10}$$

Moreover, because they are mutually tangent, we also have

$$(c\overline{c} + r_1 - r_2)^2 = 4c\overline{c}r_1 \quad \text{for } c := c_2 - c_1 \tag{11}$$

by Lemma 2. Note that $c \in \mathrm{GF}(q)$, and therefore $c\overline{c} = c^2$. We write r_2 as

$$r_2 = \frac{c_2^2}{c_1^2} r_1 = \Big(\frac{c}{c_1} + 1\Big)^2 r_1$$

and apply it to equation (11):

$$\Big(\Big(\frac{c}{c_1} + 1\Big)^2 r_1 - r_1 - c^2\Big)^2 = 4c^2 r_1 \iff \Big(\Big(\frac{c^2}{c_1^2} + \frac{2c}{c_1}\Big) r_1 - c^2\Big)^2 = 4c^2 r_1.$$

Dividing both sides by c^2, which is nonzero because $B^1_{(c_1,r_1)}$ and $B^1_{(c_2,r_2)}$ are different, yields

$$\Big(c\frac{r_1 - c_1^2}{c_1^2} + \frac{2r_1}{c_1}\Big)^2 = 4r_1. \tag{12}$$

Note that $c\frac{r_1-c_1^2}{c_1^2} + \frac{2r_1}{c_1} \in \mathrm{GF}(q)$, since $c, r_1, c_1 \in \mathrm{GF}(q)$. Consequently, (12) only has a solution if r_1 is a square in $\mathrm{GF}(q)$. In view of equation (10) it is clear that r_1 is a square in $\mathrm{GF}(q)$ if and only if $\gamma\overline{\gamma}$ is a square in $\mathrm{GF}(q)$. In that case we can write equation (12) as

$$c\frac{r_1 - c_1^2}{c_1^2} = \pm 2\sqrt{r_1} - \frac{2r_1}{c_1}. \tag{13}$$

At this point we observe that $r_1 - c_1^2 \neq 0$, i.e., $\frac{(\gamma+\overline{\gamma})^2}{4\gamma\overline{\gamma}} \neq 1$. In fact, $(\gamma+\overline{\gamma})^2 = 4\gamma\overline{\gamma} \iff (\gamma-\overline{\gamma})^2 = 0 \iff \gamma = \overline{\gamma}$, but as we mentioned earlier, $\gamma^2 \neq \overline{\gamma}^2$. We can therefore rearrange (13) by solving for c:

$$c = \frac{c_1^2}{r_1 - c_1^2}\Big(\pm 2\sqrt{r_1} - \frac{2r_1}{c_1}\Big) = -\frac{2c_1\sqrt{r_1}}{\pm c_1 + \sqrt{r_1}}.$$

We use that $c_2 = c + c_1$ and get

$$c_2 = c_1 \frac{c_1 \mp \sqrt{r_1}}{c_1 \pm \sqrt{r_1}}.$$

Finally, substituting r_1 gives (9), as claimed. □

Lemma 12. *Let $B^1_{(c_1,r_1)}, B^1_{(c_2,r_2)} \in \tau(B^2_{(\gamma,0)}, B^2_{(\overline{\gamma},0)})$ with $c_1 = -\overline{c}_1$ and $c_2 = -\overline{c}_2$. The circles $B^1_{(c_1,r_1)}$ and $B^1_{(c_2,r_2)}$ are tangent if and only if $-\gamma\overline{\gamma}$ is a nonsquare in* $\mathrm{GF}(q)$ *and*

$$c_2 = c_1 \cdot \frac{2\sqrt{-\gamma\overline{\gamma}} \pm (\gamma - \overline{\gamma})}{2\sqrt{-\gamma\overline{\gamma}} \mp (\gamma - \overline{\gamma})}. \tag{14}$$

Proof. Both circles $B^1_{(c_1,r_1)}$ and $B^1_{(c_2,r_2)}$ must satisfy equation (7) from Lemma 10, i.e.

$$c_i = -\overline{c}_i, \quad r_i = c_i^2 \frac{(\gamma-\overline{\gamma})^2}{4\gamma\overline{\gamma}}, \qquad c_i \neq 0, \quad i = 1, 2. \tag{15}$$

Moreover we have again (11) as in Lemma 11. But note that this time we have $c\overline{c} = -c^2$. We write r_2 as

$$r_2 = \frac{c_2^2}{c_1^2} r_1 = \Big(\frac{c}{c_1} + 1\Big)^2 r_1.$$

Equation (11) now reads $((\frac{c}{c_1}+1)^2 r_1 - r_1 + c^2)^2 = -4c^2 r_1$, or equivalently

$$\Big(c\frac{r_1+c_1^2}{c_1^2} + \frac{2r_1}{c_1}\Big)^2 = -4r_1, \tag{16}$$

where we used that $c \neq 0$ (because $B^1_{(c_1,r_1)}$ and $B^1_{(c_2,r_2)}$ are different). We have a closer look at equation (16). For this, define

$$\iota := c\frac{r_1+c_1^2}{c_1^2} + \frac{2r_1}{c_1}.$$

Observe that $\overline{\iota} = -\iota$, which means that ι is on the circle $z + \overline{z} = 0$. This implies that in order for (16) to be solvable, we need the square root of $-4r_1$ to be on that circle as well. Since $-4r_1 \in \mathrm{GF}(q)$, the square root always exists in $\mathrm{GF}(q^2)$, and we conclude that $-r_1$ must be a nonsquare in $\mathrm{GF}(q)$. In view of (15) this is the case if and only if $-y\overline{y}$ is a nonsquare in $\mathrm{GF}(q)$. In this case, we can solve equation (16) for c and obtain

$$c = \frac{c_1^2}{r_1+c_1^2}\Big(\pm 2\sqrt{-r_1} - \frac{2r_1}{c_1}\Big) \quad \text{with} \quad \sqrt{-r_1} = c_1\frac{y-\overline{y}}{2\sqrt{-y\overline{y}}}. \tag{17}$$

We also mention here that $r_1 + c_1^2 \neq 0$, i.e. $\frac{(y-\overline{y})^2}{4y\overline{y}} \neq -1$. This follows from the condition $y^2 \neq \overline{y}^2$, because

$$(y-\overline{y})^2 = -4y\overline{y} \iff (y+\overline{y})^2 = 0.$$

Using (17) in $c_2 = c + c_1$, a short calculation yields

$$c_2 = c_1\frac{c_1 \pm \sqrt{-r_1}}{c_1 \mp \sqrt{-r_1}}.$$

If we plug in the term for $\sqrt{-r_1}$ in the previous expression, we finally get (14), as claimed. □

Lemma 13. *Let $B^1_{(c_1,r_1)}, B^1_{(c_2,r_2)} \in \tau(B^2_{(y,0)}, B^2_{(\overline{y},0)})$ with $c_1 = \overline{c}_1$ and $c_2 = -\overline{c}_2$. The circles $B^1_{(c_1,r_1)}$ and $B^1_{(c_2,r_2)}$ are tangent if and only if*

$$c_2 = \pm c_1 \cdot \frac{y-\overline{y}}{y+\overline{y}}.$$

Proof. By Lemma 10 we have

$$r_1 = c_1^2\frac{(y+\overline{y})^2}{4y\overline{y}} \quad \text{and} \quad r_2 = c_2^2\frac{(y-\overline{y})^2}{4y\overline{y}}.$$

We can write r_2 as

$$r_2 = c_2^2\Big(\frac{(y+\overline{y})^2}{4y\overline{y}} - \frac{4y\overline{y}}{4y\overline{y}}\Big) = c_2^2\Big(\frac{r_1}{c_1^2} - 1\Big).$$

Furthermore, for $c := c_2 - c_1$ we have $c\overline{c} = (c_2-c_1)(-c_2-c_1) = c_1^2 - c_2^2$. We use these relations to transform the equation $(c\overline{c} + r_1 - r_2)^2 = 4c\overline{c}r_1$ for two tangent circles of the first type (see Lemma 2). We find that

$$(c\overline{c} + r_1 - r_2)^2 - 4c\overline{c}r_1 = \Big(c_1^2 - c_2^2 + r_1 - c_2^2\Big(\frac{r_1}{c_1^2} - 1\Big)\Big)^2 - 4(c_1^2 - c_2^2)r_1 = \Big(\Big(\frac{c_2^2}{c_1^2} - 1\Big)r_1 + c_1^2\Big)^2,$$

where the last term is zero if and only if $(c_2^2 - c_1^2)r_1 + c_1^4 = 0$, which is equivalent to

$$c_2^2 = c_1^2\Big(1 - \frac{c_1^2}{r_1}\Big).$$

The desired result now follows from the fact that

$$1 - \frac{c_1^2}{r_1} = 1 - \frac{4y\overline{y}}{(y+\overline{y})^2} = \frac{(y-\overline{y})^2}{(y+\overline{y})^2}.$$

□

The following lemma is a useful observation about the restriction on y as given in Lemmas 11 and 12.

Lemma 14. (i) *$y\overline{y}$ is a square in* GF(q) *if and only if y is a square in* GF(q^2).

(ii) *$-y\overline{y}$ is a nonsquare in* GF(q) *if and only if either*

- *y is a square in* GF(q^2) *and -1 is a nonsquare in* GF(q), *or*
- *y is a nonsquare in* GF(q^2) *and -1 is a square in* GF(q).

Proof. Recall that an element $b \in \mathrm{GF}(q) \setminus \{0\}$ is a square in GF(q) if and only if $b^{\frac{q-1}{2}} = 1$. Hence, by

$$(y\overline{y})^{\frac{q-1}{2}} = \left(y^{q+1}\right)^{\frac{q-1}{2}} = 1 \iff y^{\frac{q^2-1}{2}} = 1,$$

it follows that $y\overline{y}$ is a square in GF(q) if and only if y is a square in GF(q^2), which proves (i), and (ii) is similar. □

Summarizing, we have established that every circle $B^1_{(c_1,r_1)} \in \tau(B^2_{(y,0)}, B^2_{(\overline{y},0)})$ has — under the right circumstances — four tangent circles in $\tau(B^2_{(y,0)}, B^2_{(\overline{y},0)})$.

We now show that a proper Steiner chain (in accordance with Definition 1) can only be constructed in the case of Lemma 11 or 12. If $c_1 = \overline{c}_1$ and $c_2 = -\overline{c}_2$ (or vice versa), the contact point of $B^1_{(c_1,r_1)}$ and $B^1_{(c_2,r_2)}$ lies on one of the carrier circles, which is a violation of Definition 1(iii). To see this, we consult Lemma 2, where it follows that $B^1_{(c_1,r_1)}$ touches $B^2_{(y,0)}$ at

$$\zeta_y^{(1)} = \frac{c_1\overline{y} - \overline{c}_1 y}{2\overline{y}} = c_1\frac{\overline{y} - y}{2\overline{y}}$$

and $B^2_{(\overline{y},0)}$ at

$$\zeta_{\overline{y}}^{(1)} = \frac{c_1 y - \overline{c}_1\overline{y}}{2y} = c_1\frac{y - \overline{y}}{2y}.$$

Recall that for $B^1_{(c_2,r_2)}$ as given in Lemma 13 we have

$$c_2 = -\overline{c}_2 = \pm c_1\frac{y - \overline{y}}{y + \overline{y}}. \tag{18}$$

Consequently, $B^1_{(c_2,r_2)}$ has the point

$$\zeta_y^{(2)} = \frac{c_2\overline{y} - \overline{c}_2 y}{2\overline{y}} = c_2\frac{\overline{y} + y}{2\overline{y}} = \pm c_1\frac{y - \overline{y}}{y + \overline{y}}\cdot\frac{\overline{y} + y}{2\overline{y}} = \pm c_1\frac{y - \overline{y}}{2\overline{y}}$$

in common with $B^2_{(y,0)}$, whereas it shares the point

$$\zeta_{\overline{y}}^{(2)} = \frac{c_2 y - \overline{c}_2\overline{y}}{2y} = c_2\frac{y + \overline{y}}{2y} = \pm c_1\frac{y - \overline{y}}{y + \overline{y}}\cdot\frac{y + \overline{y}}{2y} = \pm c_1\frac{y - \overline{y}}{2y}$$

with $B^2_{(\overline{y},0)}$. Depending on the sign we choose in (18), we find that either $\zeta_y^{(2)}$ corresponds to $\zeta_y^{(1)}$, or $\zeta_{\overline{y}}^{(2)}$ to $\zeta_{\overline{y}}^{(1)}$. In either case, we find a point that is a contact point of three tangent circles.

Similarly, it is easy to verify that if both c_1 and c_2 are in $z - \overline{z} = 0$ (Lemma 11) or in $z + \overline{z} = 0$ (Lemma 12), there are no points shared by more than two tangent circles.

To summarize, we conclude that if $\tau(B^2_{(y,0)}, B^2_{(\overline{y},0)})$ is non-empty, any circle in $\tau(B^2_{(y,0)}, B^2_{(\overline{y},0)})$ has exactly two tangent circles which would potentially allow the construction of a Steiner chain. In other words, if we can find a Steiner chain starting from a given circle, the chain is unique.

According to our earlier reflections, we have to consider two separate cases. We start with the case where $B^1_{(c_1,r_1)}$ and $B^1_{(c_2,r_2)}$ are given as in Lemma 11.

4.1.1 Case $c_1 = \overline{c}_1$ and $c_2 = \overline{c}_2$. Let us assume that $y\overline{y}$ is a square in GF(q). We have seen (Corollary 14) that this is equivalent to y being a square in GF(q^2). Moreover, y is a square if and only if $\overline{y}$ is a square. Therefore, we can write equation (9) from Lemma 11 as

$$c_2 = c_1\cdot\frac{2\sqrt{y}\sqrt{\overline{y}} \pm (y + \overline{y})}{2\sqrt{y}\sqrt{\overline{y}} \mp (y + \overline{y})}. \tag{19}$$

Define

$$u_1 := \sqrt{y} + \sqrt{\overline{y}}, \qquad u_2 := \sqrt{y} - \sqrt{\overline{y}}, \qquad \text{and} \qquad u := -\left(\frac{u_1}{u_2}\right)^2.$$

Then the two possibilities in (19) correspond to $c_2 = uc_1$ and $c_2 = \frac{c_1}{u}$. Observe that u is in $\mathrm{GF}(q) \setminus \{0\}$. Let k be the multiplicative order of u in $\mathrm{GF}(q) \setminus \{0\}$. Apparently, c_1 is any element of $\mathrm{GF}(q) \setminus \{0\}$, the chain of circles

$$B^1_{(c_1,r_1)} \to B^1_{(uc_1,r_2)} \to B^1_{(u^2c_1,r_3)} \to \cdots \to B^1_{(u^kc_1,r_{k+1})} = B^1_{(c_1,r_1)}$$

with

$$r_i := (u^{i-1}c_1)^2 \frac{(y+\overline{y})^2}{4y\overline{y}}$$

defined as in Lemma 10, is a Steiner chain of length k. In fact, we can build such a chain starting with any element c_1 of $\mathrm{GF}(q)\setminus\{0\}$. Consequently, if y is a square in $\mathrm{GF}(q^2)$, there are $\frac{q-1}{k}$ Steiner chains, and each chain has length k.

Since the length of the Steiner chains depends on the multiplicative order of u, we have a closer look at u. It follows from the definition that $\overline{\frac{u_1}{u_2}} = -\frac{u_1}{u_2}$, i.e. $\left(\frac{u_1}{u_2}\right)^2$ is a nonsquare in $\mathrm{GF}(q)$. Since $u = -1 \cdot \left(\frac{u_1}{u_2}\right)^2$, we have to distinguish two cases:

- If -1 is a square in $\mathrm{GF}(q)$, then u is a nonsquare in $\mathrm{GF}(q)$. In this case, the multiplicative order of u is a divisor of $q-1$, but does not divide $\frac{q-1}{2}$.
- If -1 is a nonsquare in $\mathrm{GF}(q)$, u is a square in $\mathrm{GF}(q)$, and the multiplicative order of u divides $\frac{q-1}{2}$. Note that if -1 is a nonsquare in $\mathrm{GF}(q)$, then m is odd and $p \equiv 3 \bmod 4$, hence $\frac{q-1}{2}$ is not divisible by 2, and therefore the length of the Steiner chain is odd.

4.1.2 Case $c_1 = -\overline{c}_1$ and $c_2 = -\overline{c}_2$. We assume that $-y\overline{y}$ is a nonsquare in $\mathrm{GF}(q)$ as required by Lemma 12. Recall equation (14) in said lemma:

$$c_2 = c_1 \cdot \frac{2\sqrt{-y\overline{y}} \pm (y-\overline{y})}{2\sqrt{-y\overline{y}} \mp (y-\overline{y})}. \tag{20}$$

Define

$$v_1 := y + \sqrt{-1}\sqrt{y\overline{y}}, \qquad v_2 := \sqrt{-1}y + \sqrt{y\overline{y}}, \qquad \text{and} \qquad v := \left(\frac{v_1}{v_2}\right)^2.$$

The reader may verify that the two possibilities in (20) correspond to $c_2 = vc_1$ and $c_2 = \frac{c_1}{v}$. With equation (20) it is easy to see that $v \in \mathrm{GF}(q) \setminus \{0\}$ and $v \neq 1$. We denote by k' the multiplicative order of v in $\mathrm{GF}(q) \setminus \{0\}$ and let c_1 be any of the $q-1$ elements in $B^2_{(1,0)} \setminus \{0, \infty\}$. A Steiner chain of length k' is then given by

$$B^1_{(c_1,r_1)} \to B^1_{(vc_1,r_2)} \to B^1_{(v^2c_1,r_3)} \to \cdots \to B^1_{(v^{k'}c_1,r_{k'+1})} = B^1_{(c_1,r_1)}$$

with r_i determined by Lemma 10:

$$r_i := (v^{i-1}c_1)^2 \frac{(y-\overline{y})^2}{4y\overline{y}}.$$

We can construct such a chain for any element $c_1 \neq 0$ in $z + \overline{z} = 0$, which means that there are $\frac{q-1}{k'}$ possible Steiner chains.

The length of the Steiner chains depends on the multiplicative order of v. Let us therefore have a closer look at v: We note that

$$\frac{v_1}{v_2} = \frac{2\sqrt{y\overline{y}} + \sqrt{-1}(\overline{y}-y)}{y+\overline{y}}. \tag{21}$$

By assumption, $-y\overline{y}$ is a nonsquare in $\mathrm{GF}(q)$, which means that exactly one of -1 and $y\overline{y}$ is a square in $\mathrm{GF}(q)$. By (21), we can say that if -1 is a square in $\mathrm{GF}(q)$, then $\overline{\frac{v_1}{v_2}} = -\frac{v_1}{v_2}$, and otherwise, $\overline{\frac{v_1}{v_2}} = \frac{v_1}{v_2}$. Accordingly, there are two cases (see also Lemma 14):

- If -1 is a square in $\mathrm{GF}(q)$ and y a nonsquare in $\mathrm{GF}(q^2)$, then v is a nonsquare in $\mathrm{GF}(q)$. In this case, the multiplicative order of v is a divisor of $q-1$, but does not divide $\frac{q-1}{2}$.
- If -1 is a nonsquare in $\mathrm{GF}(q)$ and y a square in $\mathrm{GF}(q^2)$, then v is a square in $\mathrm{GF}(q)$, and the multiplicative order of v divides $\frac{q-1}{2}$. By the above reasoning, the length of any Steiner chain in this case is always odd.

4.1.3 Overview. We summarize what we have shown so far. Remember that -1 is a nonsquare in $\mathrm{GF}(q)$ if and only if $q \equiv 3 \bmod 4$.

Theorem 15. *Let $B^2_{(\gamma,0)}$ and $B^2_{(\overline{\gamma},0)}$ be two different circles of the second type, i.e. $\gamma^2 \neq \overline{\gamma}^2$. Define*

$$u := \frac{2\sqrt{\gamma\overline{\gamma}} + (\gamma + \overline{\gamma})}{2\sqrt{\gamma\overline{\gamma}} - (\gamma + \overline{\gamma})} \quad \text{and} \quad v := \frac{2\sqrt{-\gamma\overline{\gamma}} + (\gamma - \overline{\gamma})}{2\sqrt{-\gamma\overline{\gamma}} - (\gamma - \overline{\gamma})},$$

and let k and k' be the multiplicative order of u and v, respectively.

(i) *If -1 is a nonsquare in $\mathrm{GF}(q)$ and*
  (a) *γ is a square in $\mathrm{GF}(q^2)$, there are $\frac{q-1}{k}$ Steiner chains of length k and $\frac{q-1}{k'}$ Steiner chains of length k'.*
  (b) *γ is a nonsquare in $\mathrm{GF}(q^2)$, there are no Steiner chains.*

(ii) *If -1 is a square in $\mathrm{GF}(q)$ and*
  (a) *γ is a square in $\mathrm{GF}(q^2)$, there are $\frac{q-1}{k}$ Steiner chains of length k each.*
  (b) *γ is a nonsquare in $\mathrm{GF}(q^2)$, there are $\frac{q-1}{k'}$ Steiner chains of length k'.*

*In (*ia*) the length of every Steiner chain is odd and a divisor of $\frac{q-1}{2}$. In (*iia*) and (*iib*) the length of the Steiner chains does not divide $\frac{q-1}{2}$.*

Note that if -1 is a square in $\mathrm{GF}(q)$, Steiner chains always exist, and exactly $q-1$ circles are part of a Steiner chain. If -1 is a nonsquare in $\mathrm{GF}(q)$ and γ is a square, then there are $2(q-1)$ circles used in Steiner chains.

4.2 The general case

Let $C_1 \neq C_2$ be two arbitrary circles with two intersection points z_1 and z_2. A Möbius transformation T mapping z_1 to 0 and z_2 to ∞ maps C_1 and C_2 to two circles of the second type, say $B^2_{(\gamma_1,0)}$ and $B^2_{(\gamma_2,0)}$. Since C_1 and C_2 are different, we have $\gamma_1\overline{\gamma}_2 - \overline{\gamma}_1\gamma_2 \neq 0$. And C_1 and C_2 carry a Steiner chain if and only if $B^2_{(\gamma_1,0)}$ and $B^2_{(\gamma_2,0)}$ carry a Steiner chain.

We observed that in order for a Steiner chain to exist, $\gamma_1\gamma_2$ must be a square in $\mathrm{GF}(q^2)$, and this is the case if and only if $\frac{\overline{\gamma}_2}{\overline{\gamma}_1}$ is a square. This allows to map the circles $B^2_{(\gamma_1,0)}$ and $B^2_{(\gamma_2,0)}$ to $B^2_{(\gamma,0)}$ and $B^2_{(\overline{\gamma},0)}$, where

$$\gamma := \sqrt{\overline{\gamma}_2/\overline{\gamma}_1},$$

and the condition $\gamma_1\overline{\gamma}_2 \neq \overline{\gamma}_1\gamma_2$ changes to $\gamma^2 \neq \overline{\gamma}^2$.

But what is the necessary condition for two *arbitrary* intersecting circles C_1, C_2 to carry a Steiner chain? This questions will now be answered using the capacitance (see Section 2). The capacitance of $B^2_{(\gamma_1,0)}$ and $B^2_{(\gamma_2,0)}$ (and hence of C_1 and C_2) is given by

$$\kappa = \frac{1}{\gamma_1\overline{\gamma}_1\gamma_2\overline{\gamma}_2}(\gamma_1\overline{\gamma}_2 + \overline{\gamma}_1\gamma_2)^2 = \frac{\overline{\gamma}_2}{\overline{\gamma}_1}\cdot\frac{\gamma_1}{\gamma_2} + 2 + \frac{\overline{\gamma}_1}{\overline{\gamma}_2}\cdot\frac{\gamma_2}{\gamma_1}.$$

Hence, if instead of formulating a condition for $\frac{\overline{\gamma}_2}{\overline{\gamma}_1}$ we can state a condition for κ, we will be able to decide for two arbitrary intersecting circles whether they may possibly carry a Steiner chain or not by looking at their capacitance. This is the motivation behind the following lemma.

Lemma 16. *$\frac{\overline{\gamma}_2}{\overline{\gamma}_1}$ is a square in $\mathrm{GF}(q^2)$ if and only if either*

- *$\kappa = 0$ and -1 is a nonsquare in $\mathrm{GF}(q)$, or*
- *$\kappa \neq 0$ is a square in $\mathrm{GF}(q)$.*

Proof. We substitute $\frac{\overline{\gamma}_2}{\overline{\gamma}_1}$ by g and write κ as

$$\kappa = \frac{g}{\overline{g}} + 2 + \frac{\overline{g}}{g} = \frac{(g+\overline{g})^2}{g\overline{g}}. \tag{22}$$

Since κ is in GF(q), its square root in GF(q^2) always exists. In particular, it is clear from (22) that if $\kappa \neq 0$, its square root is in GF(q) if and only if $g\overline{g}$ is a square in GF(q). Having a look at Corollary 14, it is evident that this is equivalent to $g = \frac{\overline{y}_2}{\overline{y}_1}$ being a square in GF(q^2).

On the other hand, if $\kappa = 0$, then $\overline{g} = -g$, which is equivalent to $g\overline{g} = -g^2$ (recall that $g \neq 0$ since $y_1\overline{y}_2 - \overline{y}_1 y_2 \neq 0$). It follows that a square root of $g\overline{g}$ is given by $\sqrt{-1}g$, and therefore $g\overline{g}$ is a square in GF(q) if and only if $\sqrt{-1}g \in$ GF(q). Since $g = -\overline{g}$, this is the same as requiring that $\sqrt{-1}$ is a nonsquare in GF(q) . With Corollary 14 we conclude that g is a square in GF(q^2) if and only if -1 is a nonsquare in GF(q). □

From now on, we assume that $\frac{\overline{y}_2}{\overline{y}_1}$ is a square in GF(q^2). In this case we can write

$$\kappa = \frac{\gamma^2}{\overline{\gamma}^2} + 2 + \frac{\overline{\gamma}^2}{\gamma^2} = \left(\frac{\gamma}{\overline{\gamma}} + \frac{\overline{\gamma}}{\gamma}\right)^2$$

where $\gamma = \sqrt{\frac{\overline{y}_2}{\overline{y}_1}}$ is a square root of $\frac{\overline{y}_2}{\overline{y}_1}$. Note that κ (and also the square root of κ) does not depend on which square root of $\frac{\overline{y}_2}{\overline{y}_1}$ we assign to γ.

At this point Theorem 15 comes into play: We saw that the existence and length of a Steiner chain depends on whether γ is a square in GF(q^2) or not. We want to characterize existence or non-existence in terms of the capacitance. To investigate this, we need to find a correlation between κ and γ being a square or a nonsquare. We consider two separate cases (compare with Lemma 16):

(i) $\kappa = 0$ and -1 is a nonsquare in GF(q) (Lemma 17), and

(ii) $\kappa \neq 0$ is a square in GF(q) (Lemma 18).

The reader may want to have a look at Theorem 20 and Table 1 already to see what we are aiming at.

Lemma 17. *If $\kappa = 0$ and -1 is a nonsquare in* GF(q)*, then γ is a square in* GF(q^2) *if and only if $p \equiv 7 \bmod 16$.*

Proof. The condition $\kappa = 0$ is equivalent to

$$\frac{\gamma}{\overline{\gamma}} + \frac{\overline{\gamma}}{\gamma} = 0 \iff \gamma^2 + \overline{\gamma}^2 = 0 \iff \gamma = \pm\sqrt{-1}\overline{\gamma}.$$

Be aware that $\gamma \notin$ GF(q), and in particular $\gamma \neq 0$, a consequence of the afore-mentioned property $\gamma^2 \neq \overline{\gamma}^2$. Multiplying both sides of the equation by γ leads to $\gamma^2 = \sqrt{-1} \cdot \gamma\overline{\gamma}$, where we omit the $\pm$-sign by using $\sqrt{-1}$ to represent both square roots of -1. If we write $\sqrt{-1}$ as $\sqrt{-1} = \frac{\gamma^2}{\gamma\overline{\gamma}}$, it is obvious that a square root of $\sqrt{-1}$ exists. We can therefore write

$$\gamma = \sqrt{\sqrt{-1}} \cdot \sqrt{\gamma\overline{\gamma}}. \tag{23}$$

Since $q \equiv 3 \bmod 4$, we have $q^2 \equiv 1 \bmod 4$ and hence 4 divides $q^2 - 1$. Thus every element in GF(q) is a fourth power in GF(q^2). In particular, $\sqrt{\gamma\overline{\gamma}}$ is a square.

So, by (23) we have that γ is a square if and only if $\sqrt{\sqrt{-1}}$ is a square. This is the case if and only if the multiplicative order of $\sqrt{\sqrt{-1}}$ is a divisor of $\frac{q^2-1}{2}$. Since -1 has multiplicative order 2, the multiplicative order of $\sqrt{\sqrt{-1}}$ is 8. This implies that γ is a square in GF(q^2) if and only if $q^2 - 1$ is divisible by 16, i.e. if and only if $q^2 \equiv 1 \bmod 16$. Since m is odd and $q \equiv 3 \bmod 4$ if follows easily that $p \equiv 7 \bmod 16$. □

Recall that $\kappa = \left(\frac{\gamma}{\overline{\gamma}} + \frac{\overline{\gamma}}{\gamma}\right)^2$. In the following lemma, we choose $\frac{\gamma}{\overline{\gamma}} + \frac{\overline{\gamma}}{\gamma}$ as the square root of κ.

Lemma 18. *Assume that $\kappa \neq 0$ is a square in* GF(q) *with square root $\sqrt{\kappa} = \frac{\gamma}{\overline{\gamma}} + \frac{\overline{\gamma}}{\gamma}$. Then:*

(i) *If -1 is a nonsquare in* GF(q)*, the following are equivalent:*
γ is a square in GF(q^2) $\iff$ *$\sqrt{\kappa} + 2$ is a square in* GF(q) $\iff$ *$-\sqrt{\kappa} + 2$ is a square in* GF(q).

(ii) *If -1 is a square in* GF(q)*, the following are equivalent:*
γ is a square in GF(q^2) $\iff$ *$\sqrt{\kappa} + 2$ is a square in* GF(q) $\iff$ *$-\sqrt{\kappa} + 2$ is a nonsquare in* GF(q).

Proof. We treat the two cases $\sqrt{\kappa} + 2$ and $-\sqrt{\kappa} + 2$ separately:

- For $\sqrt{\kappa}+2$ we have
$$\sqrt{\kappa}+2=\frac{\gamma}{\overline{\gamma}}+2+\frac{\overline{\gamma}}{\gamma}=\frac{(\gamma+\overline{\gamma})^2}{\gamma\overline{\gamma}}.$$
Note that $\gamma+\overline{\gamma}\neq 0$ as $\gamma^2\neq\overline{\gamma}^2$. Obviously, $\sqrt{\kappa}+2$ is a square in $\mathrm{GF}(q)$ if and only if $\gamma\overline{\gamma}$ is a square in $\mathrm{GF}(q)$, which is the case if and only if γ is a square in $\mathrm{GF}(q^2)$; see Corollary 14.
- Conversely, for $-\sqrt{\kappa}+2$ we can write
$$-\sqrt{\kappa}+2=-\frac{\gamma}{\overline{\gamma}}+2-\frac{\overline{\gamma}}{\gamma}=\frac{(\gamma-\overline{\gamma})^2}{-\gamma\overline{\gamma}}.$$
Note that $\gamma-\overline{\gamma}\neq 0$ as $\gamma^2\neq\overline{\gamma}^2$. Here, $-\sqrt{\kappa}+2$ is a square in $\mathrm{GF}(q)$ if and only if $-\gamma\overline{\gamma}$ is a nonsquare in $\mathrm{GF}(q)$. Again, the desired result follows with Corollary 14. □

Remark 19. If $\sqrt{\kappa}$ is a square root of κ and -1 is a nonsquare in $\mathrm{GF}(q)$, then $\sqrt{\kappa}+2$ is a square in $\mathrm{GF}(q)$ if and only if γ is a square in $\mathrm{GF}(q^2)$ (Case (i) of Lemma 18). On the other hand, if -1 is a square in $\mathrm{GF}(q)$ (Case (ii) of Lemma 18), exactly one of $\sqrt{\kappa}+2$ and $-\sqrt{\kappa}+2$ is a square in $\mathrm{GF}(q)$. A Steiner chain in this case always exists: we are either in Case (iia) or in Case (iib) of Theorem 15.

What we still lack is a condition for the length of the Steiner chains in case they exist. For this, we rewrite u and v in Theorem 15 as follows:

$$u=\frac{2+\frac{\gamma+\overline{\gamma}}{\sqrt{\gamma\overline{\gamma}}}}{2-\frac{\gamma+\overline{\gamma}}{\sqrt{\gamma\overline{\gamma}}}}\quad\text{and}\quad v=\frac{2+\frac{\gamma-\overline{\gamma}}{\sqrt{-\gamma\overline{\gamma}}}}{2-\frac{\gamma-\overline{\gamma}}{\sqrt{-\gamma\overline{\gamma}}}}.$$

Note that

$$\left(\frac{\gamma\pm\overline{\gamma}}{\sqrt{\pm\gamma\overline{\gamma}}}\right)^2=\pm\frac{\gamma}{\overline{\gamma}}+2\pm\frac{\overline{\gamma}}{\gamma}=\pm\sqrt{\kappa}+2.$$

Apparently, u and v (or $\frac{1}{u}$ and $\frac{1}{v}$, depending on which square root of $\pm\sqrt{\kappa}+2$ we take) correspond to

$$w^{\pm}:=\frac{2+\sqrt{\pm\sqrt{\kappa}+2}}{2-\sqrt{\pm\sqrt{\kappa}+2}}.$$

In particular, if $\kappa=0$, we have $w^{\pm}=\frac{2+\sqrt{2}}{2-\sqrt{2}}=3+2\sqrt{2}$. Our results from Section 4.2 combined with Theorem 15 are now summarized in the following

Theorem 20. *Let C_1 and C_2 be two intersecting circles in $\mathbb{M}(q)$, where $q=p^m$ for an odd prime p. Let $\kappa:=\mathrm{cap}(C_1,C_2)$ be the capacitance of C_1, C_2, and $\sqrt{\kappa}$ any square root of κ. If $\sqrt{\kappa}\in\mathrm{GF}(q)$, we additionally define*

$$w^{\pm}:=\frac{2+\sqrt{\pm\sqrt{\kappa}+2}}{2-\sqrt{\pm\sqrt{\kappa}+2}}.$$

Then, the circles C_1 and C_2 carry a Steiner chain if and only if one of the following three conditions is satisfied:

(i) *$\kappa=0$, m is odd, and $p\equiv 7 \bmod 16$.*
In this case there are $2\frac{q-1}{k}$ Steiner chains, whose length k is given by the multiplicative order of $3+2\sqrt{2}$.

(ii) *$\kappa\neq 0$, $\sqrt{\kappa}\in\mathrm{GF}(q)$, -1 is a nonsquare in $\mathrm{GF}(q)$, and $\sqrt{\kappa}+2$ is a square in $\mathrm{GF}(q)$.*
There are $\frac{q-1}{k^+}$ Steiner chains of length k^+ and $\frac{q-1}{k^-}$ Steiner chains of length k^-, where k^+ and k^- are the multiplicative orders of w^+ and w^-, respectively.

(iii) *$\kappa\neq 0$, $\sqrt{\kappa}\in\mathrm{GF}(q)$, and -1 is a square in $\mathrm{GF}(q)$.*
There are $\frac{q-1}{k}$ Steiner chains of length k each, where k is the multiplicative order of w^+ if $\sqrt{\kappa}+2$ is a square in $\mathrm{GF}(q)$, and the multiplicative order of w^- otherwise.

In (i) *and* (ii)*, the length of the chains is odd and a divisor of $\frac{q-1}{2}$, whereas the length of the chains in Case* (iii) *does not divide $\frac{q-1}{2}$.*

Case	$q \equiv 3 \mod 4$		$q \equiv 1 \mod 4$
Condition	$\kappa = 0$ and $p \equiv 7 \mod 16$.	$\kappa \neq 0$ is a square in GF(q) and $\sqrt{\kappa}+2$ is a square in GF(q).	$\kappa \neq 0$ is a square in GF(q).
Result	There are $2\frac{q-1}{k}$ chains of length k.	There are $\frac{q-1}{k^+}$ chains of length k^+ and $\frac{q-1}{k^-}$ chains of length k^-.	There are $\frac{q-1}{k}$ chains of length k.
Comment	k is the multiplicative order of $3+2\sqrt{2}$.	k^+ is the multiplicative order of w^+ and k^- is the multiplicative order of w^-.	k is the multiplicative order of $w^\pm$, where the sign is chosen such that $\pm\sqrt{\kappa}+2$ is a square in GF(q).
Specifics	The length of the chains is odd and divides $\frac{q-1}{2}$.		The length of the chains divides $q-1$ but does not divide $\frac{q-1}{2}$.

Table 1: Overview of Steiner chains for intersecting carrier circles in $\mathbb{M}(q)$

Example. If $\mathbb{M}(31)$ is constructed over the pair of finite fields GF(31) and GF(31)(α) with $\alpha = \sqrt{-1}$, one can verify by Lemma 2 that the circles $B^1_{(3\alpha+8,14)}$ and $B^2_{(5\alpha+12,17)}$ are intersecting, and we compute that their capacitance κ equals 2.

A square root of κ is given by $\sqrt{\kappa} = 8$. Moreover, we can determine the square roots $\sqrt{\sqrt{\kappa}+2} = 14$ and $\sqrt{-\sqrt{\kappa}+2} = 5$. Obviously, all the requirements for the existence of a Steiner chain as stated in Theorem 20(ii) are satisfied. To determine the length of the Steiner chains, we have a look at $w^\pm$:

$$w^+ = \frac{2+14}{2-14} = \frac{16}{19} = 9, \qquad w^- = \frac{2+5}{2-5} = \frac{7}{28} = 8.$$

The multiplicative orders of $w^+ = 9$ and $w^- = 8$ are 15 and 5, respectively. Accordingly, $B^1_{(3\alpha+8,14)}$ and $B^2_{(5\alpha+12,17)}$ carry 2 Steiner chains of length 15 and 6 Steiner chains of length 5. This can be confirmed by an exhaustive search of circles, implemented in Sage. Explicit code can be found in [8].

Acknowledgements: We would like to thank the referee for his or her careful reading and the valuable remarks which greatly helped to improve this article.

References

[1] O. D. Byer, D. L. Smeltzer, A 3-D analog of Steiner's Porism. *Math. Mag.* **87** (2014), 95–99. MR3193739 Zbl 1298.51016
[2] J. L. Coolidge, *A treatise on the circle and the sphere*. Chelsea Publishing Co., Bronx, N.Y. 1971. MR0389515 Zbl 0251.50002
[3] H. S. M. Coxeter, *Introduction to geometry*. Wiley-Interscience 1989. MR990644 Zbl 0181.48101
[4] P. Dembowski, *Finite geometries*. Springer 1997. MR1434062 Zbl 0865.51004
[5] N. Hungerbühler, K. Kusejko, Steiner's porism in finite Miquelian Möbius planes. *Adv. Geom.* **18** (2018), 55–68. MR3750254 Zbl 1383.05039
[6] R. Lidl, H. Niederreiter, *Introduction to finite fields and their applications*. Cambridge Univ. Press 1986. MR860948 Zbl 0629.12016
[7] D. Pedoe, *Geometry*. Dover Publications, Inc., New York 1988. MR1017034 Zbl 0716.51002
[8] G. Villiger, *A variation of Steiner's Porism in Miquelian Möbius Planes of odd order*. Master thesis, Institute of Mathematics, University of Zürich, 2018.
[9] P. Yiu, Rational Steiner porism. *Forum Geom.* **11** (2011), 237–249. MR2877262 Zbl 1287.51002