Norbert Hungerbühler and Katharina Kusejko*

Steiner's Porism in finite Miquelian Möbius planes

DOI 10.1515/advgeom-2017-0027. Received 6 August, 2015; revised 1 April, 2016

Abstract: We investigate Steiner's Porism in finite Miquelian Möbius planes constructed over the pair of finite fields GF(q) and GF(q^2), for an odd prime power q. Properties of common tangent circles for two given concentric circles are discussed and with that, a finite version of Steiner's Porism for concentric circles is stated and proved. We formulate conditions on the length of a Steiner chain by using the quadratic residue theorem in GF(q). These results are then generalized to an arbitrary pair of non-intersecting circles by introducing the notion of capacitance, which turns out to be invariant under Möbius transformations. Finally, the results are compared with the situation in the classical Euclidean plane.

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

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

Communicated by: G. Korchmáros

Introduction

In the 19th century, the Swiss mathematician Jakob Steiner (1796–1863) discovered a beautiful result about tangent circles in the Euclidean plane, known as *Steiner's Porism*. One version reads as follows.

Theorem (Steiner's Porism). *Let $\mathcal{B}$ and $\mathcal{B}'$ be disjoint circles in the Euclidean plane. Consider a sequence of different circles $\mathcal{T}_1, \dots, \mathcal{T}_k$ which are tangent to both $\mathcal{B}$ and $\mathcal{B}'$. Moreover, let $\mathcal{T}_i$ and $\mathcal{T}_{i+1}$ be tangent for $i = 1, \dots, k-1$. If $\mathcal{T}_1$ and $\mathcal{T}_k$ are tangent as well, then there are infinitely many such chains. In particular, every chain of consecutive tangent circles closes after k steps.*

Steiner thoroughly investigated such chains and found many nice properties. For example, he could prove that the tangent points of the circles $\mathcal{T}_1, \dots, \mathcal{T}_k$ lie on a circle and that their centers lie on a conic whose foci are the centers of the initial circles $\mathcal{B}$ and $\mathcal{B}'$. He studied conditions for such a chain to close after k steps in terms of the radii and the distance between the centers of $\mathcal{B}$ and $\mathcal{B}'$. The interested reader can refer to [2], [8] or [3] for more information on Steiner's original result. In recent years, some refinements and generalizations of Steiner's Porism were studied. For example, in [9] Steiner chains with rational radii are discussed, and in [1] a three-dimensional analogue of Steiner's Porism is presented.

Porisms in finite geometry have not been investigated to the same extent as in the Euclidean case. In particular, as far as we know, Steiner's Porism was not yet considered in finite Möbius planes. However, chains of touching circles with a different arrangement have been investigated in [10].

Möbius planes consist of points $\mathbb{P}$ and circles $\mathbb{B}$ which satisfy three axioms. First, there needs to be a unique circle through three given points. Second, there exists a unique tangent circle through a point on a given circle and a point not on this circle. Finally, a richness axiom ensures that the plane is not trivial. More precisely, the three axioms read as follows.

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

Norbert Hungerbühler, ETH Zürich, Department of Mathematics, Rämistrasse 101, 8092 Zürich, Switzerland, email: norbert.hungerbuehler@math.ethz.ch

***Corresponding author: Katharina Kusejko,** Universität Zürich, Institut für Medizinische Virologie, Winterthurerstrasse 190, 8057 Zürich, Switzerland, e-mail: katharina.kusejko@usz.ch

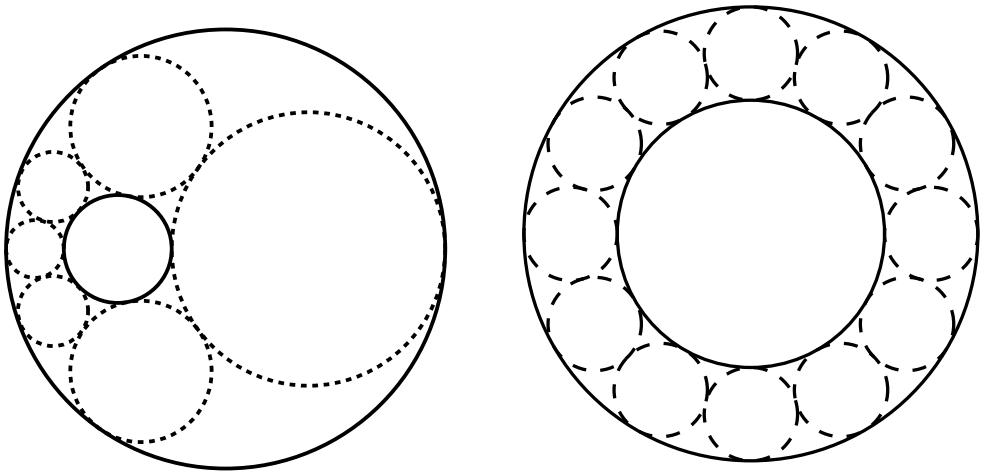

Figure 1: Two examples of Steiner chains in the Euclidean plane.

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

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

In the present paper, we look at Steiner's Porism in Miquelian Möbius planes. They are the classical finite models for the Möbius axioms and are constructed over the finite field $\mathrm{GF}(q)$ of order q, where q is an odd prime power. The resulting plane is denoted by $\mathbb{M}(q)$, the details are explained in the preliminaries. We start with two circles $\mathcal{B}_a$ and $\mathcal{B}_b$ with common center 0 and radii a and b. We look for conditions and properties of their potential common tangent circles. Concerning this question, we find the following:

Theorem (cf. Theorem 2.1). *If $b/a \neq 1$ is a square in $\mathrm{GF}(q)$, then $\mathcal{B}_a$ and $\mathcal{B}_b$ have exactly $2(q+1)$ common tangent circles. Moreover, these tangent circles are divided into two groups of $q+1$ common tangent circles, each group having the same radius. If $b/a \neq 1$ is a nonsquare in $\mathrm{GF}(q)$, then $\mathcal{B}_a$ and $\mathcal{B}_b$ do not have any common tangent circles.*

We are interested in finding a condition for the existence of Steiner chains, i.e. chains of circles $T_1, \ldots, T_k$ of the same radius which are tangent to both $\mathcal{B}_a$ and $\mathcal{B}_b$ and each T_i, $1 \leq i \leq k$ is tangent to its neighbors in the chain.

In the classical Euclidean plane, conditions on the length of Steiner chains are well-known. For two circles with a common center and radii 1 and R, one can construct a Steiner chain of length $k \geq 3$ which wraps w times around the smaller circle, if and only if

$$R = \frac{1 + \sin(\varphi)}{1 - \sin(\varphi)},$$

where $\varphi = \frac{w\pi}{k}$. In particular, for every $k \geq 3$ a Steiner chain of length k can be constructed. We ask for such conditions in the finite case and obtain the following result:

Theorem (cf. Theorem 4.2). *Let $\mathcal{B}_1$ and $\mathcal{B}_{a^2}$ be two circles in $\mathbb{M}(q)$. If $q \equiv -1 \pmod 4$, exactly one Steiner chain can be constructed with $\mathcal{B}_1$ and $\mathcal{B}_{a^2}$. If $q \equiv 1 \pmod 4$, either two or zero Steiner chains can be constructed with $\mathcal{B}_1$ and $\mathcal{B}_{a^2}$, depending on whether or not a is a square in $\mathrm{GF}(q)$. Moreover, only divisors of $q+1$ can serve as the length of a Steiner chain.*

In the last section, we introduce the notion of capacitance for a pair of circles and prove that this quantity is invariant under Möbius transformations. This fact allows to formulate a criterion for the existence of proper Steiner chains of length k for an arbitrary pair of non-intersecting circles. Finally, the results are compared to the conditions on Steiner chains in the Euclidean plane.

1 Preliminaries

We describe an explicit construction of finite Miquelian Möbius planes using finite fields. For that we need to recall some properties of finite fields $\mathrm{GF}(q)$, where q is an odd prime power.

An element $a \in \mathrm{GF}(q)$ is called a *square* in $\mathrm{GF}(q)$ if there exists some $b \in \mathrm{GF}(q)$ with $a = b^2$. All other elements in $\mathrm{GF}(q)$ are called *nonsquares* in $\mathrm{GF}(q)$. Exactly half of the elements in $\mathrm{GF}(q) \setminus \{0\}$ are squares. Note that the squares of $\mathrm{GF}(q)$ form a subgroup of $\mathrm{GF}(q)$, but the nonsquares do not. In particular, multiplying two nonsquares in $\mathrm{GF}(q)$ gives a square and multiplying a square and a nonsquare in $\mathrm{GF}(q)$ gives a nonsquare.

For any nonsquare δ in $\mathrm{GF}(q)$, we can construct an extension field of $\mathrm{GF}(q)$ by adjoining some element α with $\alpha^2 = \delta$ to $\mathrm{GF}(q)$. The elements in the extension field $\mathrm{GF}(q)(\alpha)$ are of the form $x + \alpha y$ for $x, y \in \mathrm{GF}(q)$. Note that all elements of $\mathrm{GF}(q)$ are squares in $\mathrm{GF}(q)(\alpha)$. To see this, take some element $x \in \mathrm{GF}(q)$. If x is a square in $\mathrm{GF}(q)$, it is clearly a square in $\mathrm{GF}(q)(\alpha)$ as well. If x is a nonsquare in $\mathrm{GF}(q)$, then δx is a square in $\mathrm{GF}(q)$ and hence $\delta x = y^2$ which leads to $x = \alpha^{-2} y^2$, i.e. x is a square in $\mathrm{GF}(q)(\alpha)$.

Since $\mathrm{GF}(q)(\alpha)$ is isomorphic to any field with q^2 elements, we denote it by $\mathrm{GF}(q^2)$.

For $z \in \mathrm{GF}(q^2)$ define the *conjugate element* of $z = x + \alpha y$ over $\mathrm{GF}(q)$ by

$$\overline{z} := z^q = x - \alpha y.$$

Note that $z = \overline{z}$ if and only if $z \in \mathrm{GF}(q)$. Define the *trace* of z over $\mathrm{GF}(q)$ by

$$\mathrm{Tr}_{\mathrm{GF}(q^2)/\,\mathrm{GF}(q)}(z) := z + \overline{z} = 2x \in \mathrm{GF}(q)$$

and the *norm* of z over $\mathrm{GF}(q)$ by

$$\mathrm{N}_{\mathrm{GF}(q^2)/\,\mathrm{GF}(q)}(z) := z\overline{z} = x^2 - \delta y^2 \in \mathrm{GF}(q).$$

We omit the subscript $\mathrm{GF}(q^2)/\,\mathrm{GF}(q)$ for notational convenience. Recall that $\mathrm{Tr}(z)$ and $\mathrm{N}(z)$ are always in $\mathrm{GF}(q)$, but unlike with the complex numbers $\mathrm{N}(z)$ can be a nonsquare. Furthermore, $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ and $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$. For more background on finite fields see [7].

We now describe the finite Miquelian Möbius plane constructed over the pair of finite fields $\mathrm{GF}(q)$ and $\mathrm{GF}(q^2)$. This plane 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 ∞. We distinguish two different types of circles. For circles of the first type, we consider solutions of the equation $\mathrm{N}(z - s) = c$, i.e.

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

for $s \in \mathrm{GF}(q^2)$ and $c \in \mathrm{GF}(q)\backslash\{0\}$. It can easily be seen that there are $q + 1$ points in $\mathrm{GF}(q^2)$ on every circle (1). Moreover, there are $q^2(q - 1)$ circles of the first type. For circles of the second type, we consider the equation $\mathrm{Tr}(\overline{s}z) = c$, i.e.

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

for $s \in \mathrm{GF}(q^2)\backslash\{0\}$ and $c \in \mathrm{GF}(q)$. For every such choice of s and c, Equation (2) has q solutions in $\mathrm{GF}(q^2)$. To obtain circles of the second type, we take those q solutions together with ∞. There are $(q^2 - 1)q$ choices for s and c, but scaling with any element of $\mathrm{GF}(q)\backslash\{0\}$ leads to the same circle. Hence there are $q(q + 1)$ circles of the second type. There are $q^3 + q$ circles in total and on each circle there are $q + 1$ points. This can also be seen by (M1), as three points uniquely define a circle. Now let $a, b, c, d \in \mathrm{GF}(q^2)$ such that $ad - bc \neq 0$. The map μ defined by

$$\mu : \mathbb{M}(q) \to \mathbb{M}(q), \mu(z) = \begin{cases} \frac{az+b}{cz+d} & \text{if } z \neq \infty \text{ and } cz + d \neq 0 \\ \infty & \text{if } z \neq \infty \text{ and } cz + d = 0 \\ \frac{a}{c} & \text{if } z = \infty \text{ and } c \neq 0 \\ \infty & \text{if } z = \infty \text{ and } c = 0 \end{cases}$$

is called a *Möbius transformation* of $\mathbb{M}(q)$. Every Möbius transformation is an automorphism of $\mathbb{M}(q)$. A Möbius transformation of the form $\mu(z) = 1/\overline{z}$ is an *inversion* in the unit circle $z\overline{z} = 1$, which means

that the unit circle is fixed under μ. Möbius planes in which for every circle there exists an inversion are called inversive Möbius planes. In [4] it is shown that the finite inversive Möbius planes are exactly the finite Miquelian Möbius planes.

Note that the group of all Möbius transformations is sharply triply transitive, i.e. there is a unique Möbius transformation mapping any three points into any other three given points. For more background information on finite Möbius planes, one can refer to [5].

2 Steiner's Theorem in $\mathbb{M}(q)$

For a circle of the first type $\mathcal{B}^1_{(s,c)}$, we refer to s as the *center* of $\mathcal{B}^1_{(s,c)}$, and c is the square of the *radius*. Note that the radius, which is either square root of c, is not necessarily an element of $\mathrm{GF}(q)$. Two circles of the first type are called *concentric*, if they have the same center. Without loss of generality, we can assume that two concentric circles have center 0, since the Möbius transformation $\mu\colon \mathbb{M}(q) \to \mathbb{M}(q)$ with $\mu(z) = z - s$ maps any two concentric circles with center s to two concentric circles with center 0. In this section we henceforth consider two concentric circles with center 0, i.e. circles $\mathcal{B}^1_{(0,a)}$ and $\mathcal{B}^1_{(0,b)}$ for $a, b \in \mathrm{GF}(q) \setminus \{0\}$. For notational convenience, let us define

$$\mathcal{B}_a := \mathcal{B}^1_{(0,a)}$$

for all $a \in \mathrm{GF}(q) \setminus \{0\}$.

To obtain more insight into the geometrical properties of the circles, we use Cartesian coordinates in this section, where $z = x + \alpha y$ represents the point (x, y) and $\bar{z}$ the point $(x, -y)$. The circle $\mathcal{B}_{a^2}$ is then given by

$$\mathcal{B}_{a^2} : x^2 - \delta y^2 = a^2,$$

where δ is a nonsquare in $\mathrm{GF}(q)$. Any such circle intersects the x-axis, i.e. the circle of the second type given by $y = 0$, in the two points $(\pm a, 0)$. Now consider the unit circle $\mathcal{B}_1$ given by $x^2 - \delta y^2 = 1$ and the point $(1, 0)$. It is an easy exercise to show that there are exactly two circles which are tangent to both $\mathcal{B}_1$ and $\mathcal{B}_{a^2}$ in the point $(1, 0)$. The first circle has center $\left(\frac{a+1}{2}, 0\right)$ and radius $\frac{a-1}{2}$, the other one has center $\left(\frac{-a+1}{2}, 0\right)$ and radius $\frac{a+1}{2}$. Figure 2 page shows those two common tangent circles.

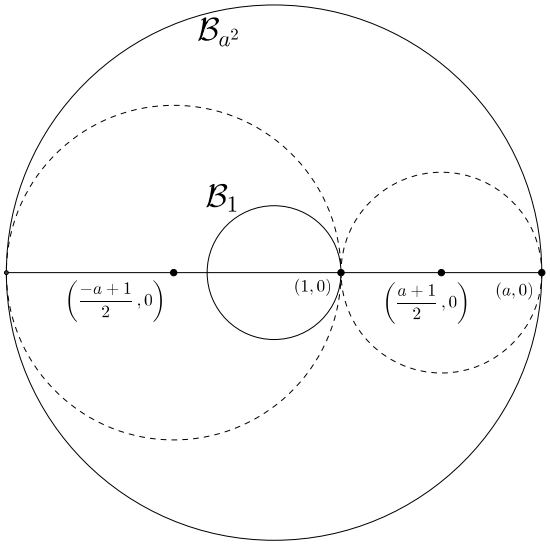

Figure 2: Common tangent circles of $\mathcal{B}_1$ and $\mathcal{B}_{a^2}$

Now consider any $(q+1)$th root of unity P, i.e. an element in $\mathrm{GF}(q^2)$ which satisfies $P^{q+1} = 1$. Since $P\overline{P} = P^{q+1}$, the rotation given by $z \mapsto Pz$ fixes both circles $\mathcal{B}_1$ and $\mathcal{B}_{a^2}$. Moreover, this rotation is a Möbius transformation and hence takes common tangent circles of $\mathcal{B}_1$ and $\mathcal{B}_{a^2}$ again into common tangent circles of $\mathcal{B}_1$ and $\mathcal{B}_{a^2}$. In particular, there are two circles tangent to $\mathcal{B}_1$ at the point P that are also tangent to $\mathcal{B}_{a^2}$, one in the point aP and the other in the point $-aP$. Note that we use the parameter a^2 as subscript, as we need it to be a square in $\mathrm{GF}(q)$ for the circles $\mathcal{B}_1$ and $\mathcal{B}_{a^2}$ to have common tangent circles.

For $a \in \mathrm{GF}(q) \setminus \{0\}$, let

$$\tau(a) := \{g \in \mathbb{B} : |\mathcal{B}_a \cap g| = 1\}$$

denote the set of all tangent circles of $\mathcal{B}_a$ and

$$\tau(a, b) := \tau(a) \cap \tau(b)$$

the set of all common tangent circles of $\mathcal{B}_a$ and $\mathcal{B}_b$. The following lemma summarizes what we just discussed.

Lemma 2.1. *If $b/a \neq 1$ is a square in $\mathrm{GF}(q)$, then $|\tau(a, b)| = 2(q+1)$, otherwise $|\tau(a, b)| = 0$.*

The $2(q+1)$ common tangent circles of $\mathcal{B}_1$ and $\mathcal{B}_{a^2}$ partition into two sets. Let P again be a fixed $(q+1)$th root of unity. There is one set of $q+1$ common tangent circles with radius $\frac{a-1}{2}$ and tangent to $\mathcal{B}_1$ in the points P^j and tangent to $\mathcal{B}_{a^2}$ in the points aP^j, for $j = 0, \dots, q$. The other $q+1$ common tangent circles of $\mathcal{B}_1$ and $\mathcal{B}_{a^2}$ have radius $\frac{a+1}{2}$ and are tangent to $\mathcal{B}_1$ in the points P^j and tangent to $\mathcal{B}_{a^2}$ in the points $-aP^j$, for $j = 0, \dots, q$.

Now we want to construct Steiner chains using the common tangent circles of two concentric circles $\mathcal{B}_1$ and $\mathcal{B}_{a^2}$. Note again that the following discussion already covers all cases for two concentric circles $\mathcal{B}_a$ and $\mathcal{B}_b$ with $a, b \in \mathrm{GF}(q)$; to see this, look at the Möbius transformation $\mu(z) = z/\eta$ for $\eta \in \mathrm{GF}(q^2)$ such that $\eta\overline{\eta} = a$. Note that such an η always exists by the properties of the norm map. Then μ maps the circles $\mathcal{B}_a$ and $\mathcal{B}_b$ to $\mathcal{B}_1$ and $\mathcal{B}_{b/a}$, respectively.

A Steiner chain of *length* $k \geq 3$ for $\mathcal{B}_1$ and $\mathcal{B}_{a^2}$ is a chain of k different circles $T_1, \dots, T_k$ in $\tau(1, a^2)$ such that $|T_i \cap T_{i+1}| = 1$ for $i = 1, \dots, k-1$ and $|T_k \cap T_1| = 1$. Moreover, all circles T_i, $i = 1, \dots, k$ need to be of the form

$$T_i = \mathcal{B}^1_{(s_i, c)}.$$

Note that all these circles T_i have the same radius, only their centers are shifted. One could define degenerate Steiner chains as well by allowing circles with different radii. In this case, we always obtain a degenerate chain for $\mathcal{B}_1$ and $\mathcal{B}_{a^2}$ by considering

$$\mathcal{B}^1_{(\frac{a+1}{2}, \frac{a-1}{2})} \to \mathcal{B}^1_{(\frac{a-1}{2}, \frac{a+1}{2})} \to \mathcal{B}^1_{(\frac{-a-1}{2}, \frac{a-1}{2})} \to \mathcal{B}^1_{(\frac{-a+1}{2}, \frac{a+1}{2})} \to \mathcal{B}^1_{(\frac{a+1}{2}, \frac{a-1}{2})}.$$

Theorem 2.2. *If there are two common tangent circles of $\mathcal{B}_1$ and $\mathcal{B}_{a^2}$ with the same radius which are tangent to each other, then a Steiner chain of length $k \geq 3$ for some k dividing $q+1$ can be constructed.*

Proof. We start with two such common tangent circles T_1 and T_2 of $\mathcal{B}_1$ and $\mathcal{B}_{a^2}$ with the same radius and $|T_1 \cap T_2| = 1$. For some root of unity P, the rotation $z \mapsto Pz$ takes the pair (T_1, T_2) to the pair (T_2, T_3), which is again a pair of common tangent circles of $\mathcal{B}_1$ and $\mathcal{B}_{a^2}$ which are tangent to each other. We can repeat this rotation k times, for k a divisor of $q+1$ and see that we finally end up with the pair (T_k, T_1), which is a pair of common tangent circles of $\mathcal{B}_1$ and $\mathcal{B}_{a^2}$ with $|T_1 \cap T_k| = 1$. In other words, we just constructed a Steiner chain of length k. □

Now we obtain our finite version of Steiner's Theorem.

Theorem 2.3. *Consider the circles $\mathcal{B}_1$ and $\mathcal{B}_{a^2}$ and assume that we can construct a Steiner chain starting with a point P on $\mathcal{B}_1$. Then a Steiner chain of the same length can be constructed starting with any other point on $\mathcal{B}_1$.*

Proof. This is immediate by using again a rotation by a root of unity. □

3 The plane $\mathbb{M}(5)$

We have a closer look at the Möbius plane $\mathbb{M}(5)$ constructed over $\mathrm{GF}(5)(\alpha)$ with $\alpha^2 = 3$, as described in the preliminaries. Consider the two circles

$$\mathcal{B}_1 := \mathcal{B}^1_{(0,1)} = \{1, 3+\alpha, 2+\alpha, 4, 2+4\alpha, 3+4\alpha\} \quad \text{and} \quad \mathcal{B}_4 := \mathcal{B}^1_{(0,4)} = \{2, 1+2\alpha, 4+2\alpha, 3, 4+3\alpha, 1+3\alpha\}.$$

Since $\frac{4}{1} = 2^2$ is a square, the two circles have exactly 12 common tangent circles. which are given by

$$\begin{aligned}
\mathcal{T}_1 &:= \mathcal{B}^1_{(4,4)} = \{1, 2, 2\alpha, 3+2\alpha, 3\alpha, 3+3\alpha\}\\
\mathcal{T}_2 &:= \mathcal{B}^1_{(2+\alpha,4)} = \{\alpha, 4+\alpha, 1+3\alpha, 3+3\alpha, 1+4\alpha, 3+4\alpha\}\\
\mathcal{T}_3 &:= \mathcal{B}^1_{(3+\alpha,4)} = \{\alpha, 1+\alpha, 2+3\alpha, 4+3\alpha, 2+4\alpha, 4+4\alpha\}\\
\mathcal{T}_4 &:= \mathcal{B}^1_{(1,4)} = \{3, 4, 2\alpha, 2+2\alpha, 3\alpha, 2+3\alpha\}\\
\mathcal{T}_5 &:= \mathcal{B}^1_{(3+4\alpha,4)} = \{2+\alpha, 4+\alpha, 2+2\alpha, 4+2\alpha, 4\alpha, 1+4\alpha\}\\
\mathcal{T}_6 &:= \mathcal{B}^1_{(2+4\alpha,4)} = \{1+\alpha, 3+\alpha, 1+2\alpha, 3+2\alpha, 4\alpha, 4+4\alpha\}
\end{aligned}$$

and

$$\begin{aligned}
\mathcal{T}_7 &:= \mathcal{B}^1_{(1+3\alpha,1)} = \{3+2\alpha, 4+2\alpha, 3\alpha, 2+3\alpha, 3+4\alpha, 4+4\alpha\}\\
\mathcal{T}_8 &:= \mathcal{B}^1_{(4+3\alpha,1)} = \{1+2\alpha, 2+2\alpha, 3\alpha, 3+3\alpha, 1+4\alpha, 2+4\alpha\}\\
\mathcal{T}_9 &:= \mathcal{B}^1_{(3,1)} = \{2, 4, \alpha, 1+\alpha, 4\alpha, 1+4\alpha\}\\
\mathcal{T}_{10} &:= \mathcal{B}^1_{(4+2\alpha,1)} = \{1+\alpha, 2+\alpha, 2\alpha, 3+2\alpha, 1+3\alpha, 2+3\alpha\}\\
\mathcal{T}_{11} &:= \mathcal{B}^1_{(1+2\alpha,1)} = \{3+\alpha, 4+\alpha, 2\alpha, 2+2\alpha, 3+3\alpha, 4+3\alpha\}\\
\mathcal{T}_{12} &:= \mathcal{B}^1_{(2,1)} = \{1, 3, \alpha, 4+\alpha, 4\alpha, 4+4\alpha\}.
\end{aligned}$$

Note that $\mathcal{T}_1$ is tangent to $\mathcal{B}_1$ in 1 and tangent to $\mathcal{B}_4$ in 2. Next, consider $\mathcal{T}_2$, which is tangent to $\mathcal{B}_1$ in $3+4\alpha$ and tangent to $\mathcal{B}_4$ in $1+3\alpha$. Note that $\mathcal{T}_1$ and $\mathcal{T}_2$ only intersect in $3+3\alpha$, i.e. they are tangent. Having a closer look at $\mathcal{T}_2$, we see that only two of the 12 circles above are tangent to $\mathcal{T}_2$ in points not on $\mathcal{B}_1$ or $\mathcal{B}_4$, namely $\mathcal{T}_1$, which we already considered, and $\mathcal{T}_3$, which is tangent to $\mathcal{T}_2$ in α. Apparently, from now on, there is a unique way of constructing a chain of common tangent circles of $\mathcal{B}_1$ and $\mathcal{B}_4$. Proceeding, we find that $\mathcal{T}_4$ is tangent to $\mathcal{T}_3$ in $2+3\alpha$. Then $\mathcal{T}_5$ is tangent to $\mathcal{T}_4$ in $2+2\alpha$. Finally, we find that $\mathcal{T}_6$ is tangent to $\mathcal{T}_5$ in 4α and also $\mathcal{T}_1$ is tangent to $\mathcal{T}_6$ in $3+2\alpha$, which closes the chain of circles.

Note that those six tangent points lie on a circle itself, namely on

$$\mathcal{B}_2 := \mathcal{B}^1_{(0,2)} = \{\alpha, 2+2\alpha, 3+2\alpha, 2+3\alpha, 3+3\alpha, 4\alpha\}.$$

Summarizing, we denote this chain by

$$\mathcal{T}_1 \xrightarrow{3+3\alpha} \mathcal{T}_2 \xrightarrow{\alpha} \mathcal{T}_3 \xrightarrow{2+3\alpha} \mathcal{T}_4 \xrightarrow{2+2\alpha} \mathcal{T}_5 \xrightarrow{4\alpha} \mathcal{T}_6 \xrightarrow{3+2\alpha} \mathcal{T}_1.$$

Note that for the above chain, we only use six out of the twelve common tangent circles of $\mathcal{B}_1$ and $\mathcal{B}_4$, so let us start with a tangent circle not used so far, e.g. $\mathcal{T}_7$. We find the chain

$$\mathcal{T}_7 \xrightarrow{3\alpha} \mathcal{T}_8 \xrightarrow{1+4\alpha} \mathcal{T}_9 \xrightarrow{1+\alpha} \mathcal{T}_{10} \xrightarrow{2\alpha} \mathcal{T}_{11} \xrightarrow{4+\alpha} \mathcal{T}_{12} \xrightarrow{4+4\alpha} \mathcal{T}_7.$$

Again, the six tangent points form a circle, namely

$$\mathcal{B}_3 := \mathcal{B}^1_{(0,3)} = \{1+\alpha, 4+\alpha, 2\alpha, 3\alpha, 1+4\alpha, 4+4\alpha\}.$$

We proceed from here and look at the circles through two consecutive (where the order is defined by the chain before) points of $\mathcal{B}_1$ and the corresponding tangency point on $\mathcal{B}_2$. We obtain six new circles, which are all tangent to $\mathcal{B}_2$, given by

$$\begin{aligned}
\mathcal{S}_1 &:= \mathcal{B}^1_{(1+\alpha,2)} = \{1, 1+2\alpha, 3+3\alpha, 4+3\alpha, 3+4\alpha, 4+4\alpha\}\\
\mathcal{S}_2 &:= \mathcal{B}^1_{(2\alpha,2)} = \{2, 3, \alpha, 3\alpha, 2+4\alpha, 3+4\alpha\}\\
\mathcal{S}_3 &:= \mathcal{B}^1_{(4+\alpha,2)} = \{4, 4+2\alpha, 1+3\alpha, 2+3\alpha, 1+4\alpha, 2+4\alpha\}\\
\mathcal{S}_4 &:= \mathcal{B}^1_{(4+4\alpha,2)} = \{4, 1+\alpha, 2+\alpha, 1+2\alpha, 2+2\alpha, 4+3\alpha\}\\
\mathcal{S}_5 &:= \mathcal{B}^1_{(3\alpha,2)} = \{2, 3, 2+\alpha, 3+\alpha, 2\alpha, 4\alpha\}\\
\mathcal{S}_6 &:= \mathcal{B}^1_{(1+4\alpha,2)} = \{1, 3+\alpha, 4+\alpha, 3+2\alpha, 4+2\alpha, 1+3\alpha\}.
\end{aligned}$$

These six circles form a chain of tangent circles as well. Moreover, there is a unique circle, apart from $\mathcal{B}_2$, which is tangent to all of those six new circles, namely $\mathcal{B}_3$.

We can perform the same procedure once more, i.e. we consider circles through two consecutive points on $\mathcal{B}_3$ and the corresponding tangency point of the chain in consideration. We obtain six common tangent circles of $\mathcal{B}_1$ and $\mathcal{B}_4$, i.e. we have two chains including all twelve common tangent circles of of $\mathcal{B}_1$ and $\mathcal{B}_4$.

Figure 3 summarizes the above discussion, with B_4 appearing in two places because the configuration showing the two Steiner chains of six circles each cannot exist in the Euclidean plane.

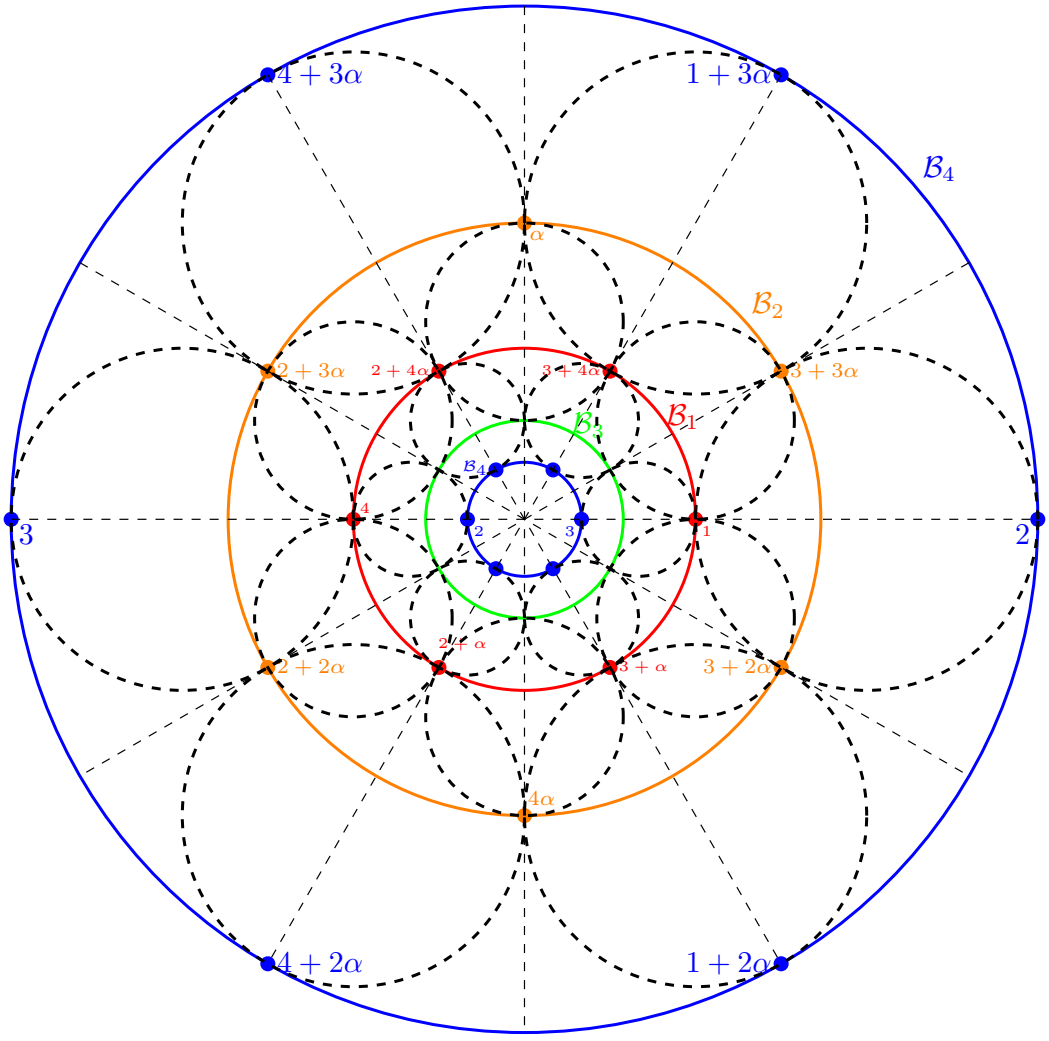

Figure 3: An example in $\mathbb{M}(5)$.

4 Existence and length of Steiner chains

In what follows, we are mainly interested in the existence of Steiner chains as well as their possible lengths.

Lemma 4.1. *Let $-a$ be a nonsquare in* $\mathrm{GF}(q)$. *Then a Steiner chain for $\mathcal{B}_1$ and $\mathcal{B}_{a^2}$ can be constructed starting with $\mathcal{B}^1_{(s,c)}$ and $\mathcal{B}^1_{(sP,c)}$ for*

$$s = \frac{a+1}{2}, \quad c = \left(\frac{a-1}{2}\right)^2 \quad \text{and} \quad P = \frac{-a^2+6a-1+4(a-1)\sqrt{-a}}{(1+a)^2}. \tag{3}$$

If $-a$ is a square in $\mathrm{GF}(q)$, *then no Steiner chain can be constructed for the pair $\mathcal{B}_1$ and $\mathcal{B}_{a^2}$.*

Proof. By the finite version of Steiner's Theorem (i.e. Theorem 2.3) we can start without loss of generality with the point 1 on $\mathcal{B}_1$ and the point a on $\mathcal{B}_{a^2}$. The parameters s and c for the circle $\mathcal{B}^1_{(s,c)}$ touching $\mathcal{B}_1$ and $\mathcal{B}_{a^2}$ in these two points are straightforward. It is well-known that if there is another circle $h \in \tau(1, a^2)$ with $|h \cap \mathcal{B}^1_{(s,c)}| = 1$, then there is a common tangent line l of those two circles through the origin. Moreover, h is obtained by a reflection of $\mathcal{B}^1_{(s,c)}$ at l. By a straightforward calculation, we find that the tangent line of $\mathcal{B}^1_{(s,c)}$ through the origin touches $\mathcal{B}^1_{(s,c)}$ in the point Q, given by

$$Q = \frac{2a}{a+1} + \sqrt{-a}\frac{a-1}{a+1}.$$

Reflecting the point 1 at the line through 0 and Q gives indeed the formula for P in (3).

If $-a$ is a square in $\mathrm{GF}(q)$, then P lies in $\mathrm{GF}(q)$. Since 1 and -1 are the only elements in $\mathrm{GF}(q)$ on $\mathcal{B}_1$, we need $-a$ to be a nonsquare in $\mathrm{GF}(q)$. □

Theorem 4.2. *Let $\mathcal{B}_1$ and $\mathcal{B}_{a^2}$ be circles of $\mathbb{M}(q)$. If $q \equiv -1 \pmod 4$, exactly one Steiner chain can be constructed with $\mathcal{B}_1$ and $\mathcal{B}_{a^2}$. If $q \equiv 1 \pmod 4$, then either two or zero Steiner chains can be constructed with $\mathcal{B}_1$ and $\mathcal{B}_{a^2}$, depending on whether or not a is a square in* $\mathrm{GF}(q)$.

Proof. In the proof of Lemma 4.1 we have seen that for $-a$ a nonsquare, a Steiner chain can be constructed starting with the circle $\mathcal{B}^1_{(s,c)}$ for $s = \frac{a+1}{2}$ and $c = \left(\frac{a-1}{2}\right)^2$. Of course, the whole proof can be done replacing a by $-a$. For $q \equiv -1 \pmod 4$, a is a square if and only if $-a$ is a nonsquare, and hence exactly one Steiner chain can be constructed. For $q \equiv 1 \pmod 4$, a is a square if and only if $-a$ is a square. Therefore, we can construct either two Steiner chains or none. □

Before we state our general result about the length of a Steiner chain, we discuss some specific cases for $\mathbb{M}(q)$ in detail. First we give a criterion for Steiner chains of length 3.

Corollary 4.3. *A Steiner chain of length 3 can be constructed for $\mathcal{B}_1$ and $\mathcal{B}_{a^2}$ in $\mathbb{M}(q)$ if and only if*

$$a = 7 + 4\sqrt{3} \in \mathrm{GF}(q)$$

and $-a$ is a nonsquare in $\mathrm{GF}(q)$. *In particular, this is possible only if $q = p^m$ for some prime $p \equiv \pm 1 \pmod{12}$.*

Proof. By Lemma 4.1 we know that $-a$ has to be a nonsquare in $\mathrm{GF}(q)$. Moreover, if $-a$ is a nonsquare in $\mathrm{GF}(q)$, we can find two circles in $\tau(1, a^2)$ which are tangent to $\mathcal{B}^1_{(s,c)}$, namely $\mathcal{B}^1_{(sP,c)}$ and $\mathcal{B}^1_{(s\overline{P},c)}$, for P given by (3). For a Steiner chain of length 3, also $\mathcal{B}^1_{(sP,c)}$ and $\mathcal{B}^1_{(s\overline{P},c)}$ need to be tangent. So we need $P^3 = 1$, or similar $P^2 = \overline{P}$ (see Figure 4).

Solving this equation for a leads to $a = 7 + 4\sqrt{3}$. This is possible only if 3 is a square in $\mathrm{GF}(q)$. It is well-known (see for example [6]) that 3 is a square in $\mathrm{GF}(q)$ only if $p \equiv \pm 1 \pmod{12}$, which gives a necessary condition for q. □

Note that this already excludes the existence of a Steiner chain of length 3 in $\mathbb{M}(5)$. Indeed, we have seen in Section 3 that only Steiner chains of length 6 occur for two concentric circles in $\mathbb{M}(5)$.

In $\mathbb{M}(11)$, however, we can find Steiner chains of length 3. For this, we calculate that $a = 7 + 4\sqrt{3}$ is 5 or 9 in $\mathrm{GF}(11)$. Moreover, $-5 = 6$ as well as $-9 = 2$ are nonsquares in $\mathrm{GF}(11)$. So Steiner chains of length 3 can be constructed for $\mathcal{B}_1$ and $\mathcal{B}_3$ as well as for $\mathcal{B}_1$ and $\mathcal{B}_4$.

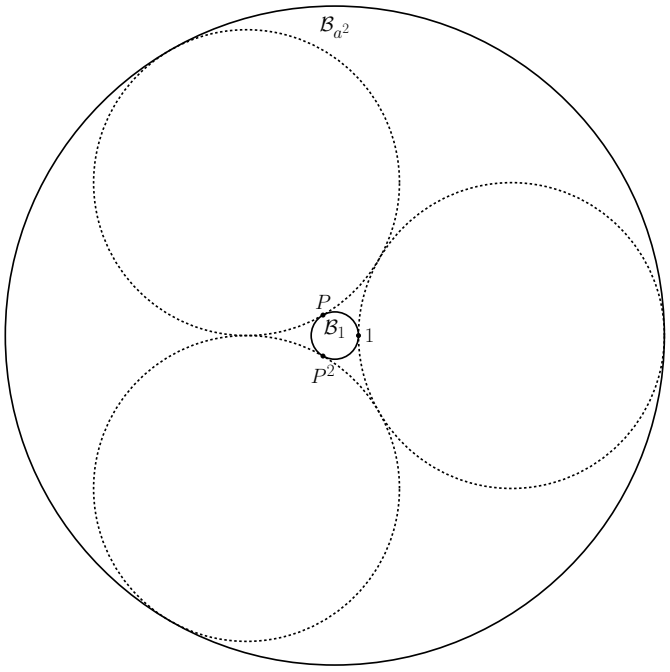

Figure 4: A Steiner chain of length 3.

Corollary 4.4. *A Steiner chain of length* 4 *can be constructed for* $\mathcal{B}_1$ *and* $\mathcal{B}_{a^2}$ *in* $\mathbb{M}(q)$ *if and only if*

$$a = 3 + 2\sqrt{2} \in \mathrm{GF}(q)$$

and $-a$ *is a nonsquare in* $\mathrm{GF}(q)$. *In particular, this is possible only if* $q = p^m$ *for some prime* $p \equiv \pm 1 \pmod 8$.

Proof. Again by Lemma 4.1, $-a$ has to be a nonsquare in $\mathrm{GF}(q)$. Moreover, if $-a$ is a nonsquare in $\mathrm{GF}(q)$, we have two circles $\mathcal{B}^1_{(sP,c)}$ and $\mathcal{B}^1_{(s\overline{P},c)}$ in $\tau(1, a^2)$, which are tangent to $\mathcal{B}^1_{(s,c)}$ with P given by (3). For a Steiner chain of length 4, we need $P^4 = 1$ or similar, $P^2 = -1$ (see Figure 5).

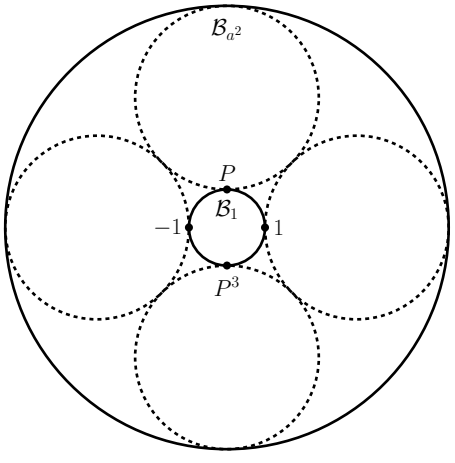

Figure 5: A Steiner chain of length 4.

Solving this equation for a gives $a = 3 + 2\sqrt{2}$. This is possible only if 2 is a square in $\mathrm{GF}(q)$. Again by [6], this implies that $q = p^m$ for some prime $p \equiv \pm 1 \pmod 8$. □

Let us have a look at $\mathbb{M}(7)$. We calculate that $a = 3 + 2\sqrt{2}$ is 2 or 4 in GF(7). Moreover, $-2 = 5$ as well as $-4 = 3$ are nonsquares in GF(7). So Steiner chains of length 4 can be constructed for $\mathcal{B}_1$ and $\mathcal{B}_2$ as well as $\mathcal{B}_1$ and $\mathcal{B}_4$. Note that 1, 2 and 4 are the only squares in GF(7), hence only Steiner chains of length 4 can be constructed using $\mathcal{B}_1$ and $\mathcal{B}_b$. Moreover, 2 is not a square in GF(11), so in $\mathbb{M}(11)$ there are no Steiner chains of length 4.

Similarly we obtain a criterion for Steiner chains of length 6.

Corollary 4.5. *A Steiner chain of length* 6 *can be constructed for* $\mathcal{B}_1$ *and* $\mathcal{B}_{a^2}$ *in* $\mathbb{M}(q)$ *if and only if* $a \in \{3, 1/3\}$ *and* -3 *is a nonsquare in* GF(q).

This criterion is different from the criterion for Steiner chains of length 3 and 4, since no square root appears in the expression for a above.

By Theorem 2.3 the existence of a Steiner chain of length 6 in $\mathbb{M}(q)$ implies that 6 divides $q + 1$. For p prime, the condition $6 \mid p + 1$ is actually equivalent with -3 being a nonsquare in GF(p), which can be seen by number theoretic calculations only. Note that in $\mathbb{M}(5)$, this gives $3^2 = 4 = 3^{-2}$, i.e. only for $\mathcal{B}_1$ and $\mathcal{B}_4$ a Steiner chain of length 6 can be constructed. Compare these results also to Section 3.

Now we look at the conditions for Steiner chains of length 5 and 8. The expressions for a become more and more difficult, since equations of higher order need to be solved. In particular, for Steiner chains of length 5 we need to solve $P^5 = 1$, and for Steiner chains of length 8 we need to solve $P^4 = -1$.

Corollary 4.6. *A Steiner chain of length* 5 *can be constructed for* $\mathcal{B}_1$ *and* $\mathcal{B}_{a^2}$ *in* $\mathbb{M}(q)$ *if and only if*

$$a = 11 - 4\sqrt{5} + 2\sqrt{50 - 22\sqrt{5}} \in \mathrm{GF}(q)$$

and $-a$ *is a nonsquare in* GF(q).

We know that if 5 is a square in GF(q), then $q = p^m$ for some prime $p \equiv \pm 1 \pmod 5$, which gives a necessary, but not sufficient condition for the existence of Steiner chains of length 5.

Corollary 4.7. *A Steiner chain of length* 8 *can be constructed for* $\mathcal{B}_1$ *and* $\mathcal{B}_{a^2}$ *in* $\mathbb{M}(q)$ *if and only if*

$$a = 7 - 4\sqrt{2} + 2\sqrt{2(10 - 7\sqrt{2})} \in \mathrm{GF}(q)$$

and $-a$ *is a nonsquare in* GF(q).

Note that 2 has to be a square, similar to the condition for Steiner chains of length 4. This is not surprising, since 8 is a multiple of 4.

Now we are ready to give a condition for Steiner chains of length $k \geq 3$.

Theorem 4.8. *Let* $a \in \mathrm{GF}(q)$. *A Steiner chain of length* $k \geq 3$ *can be constructed for* $\mathcal{B}_1$ *and* $\mathcal{B}_{a^2}$ *in* $\mathbb{M}(q)$ *if and only if the following conditions are satisfied:*

(1) $-a$ *is a nonsquare in* GF(q)*;*

(2) a *solves the equation* $P^k = 1$ *where* P *is given by*

$$P = \frac{-a^2 + 6a - 1 + 4(a-1)\sqrt{-a}}{(1+a)^2} \tag{4}$$

but $P^l \neq 1$ *for* $1 \leq l \leq k - 1$.

Proof. Assume that there exists a Steiner chain of length k. By Lemma 4.1, $-a$ has to be a nonsquare in GF(q) to obtain two circles $\mathcal{B}^1_{(sP,c)}$ and $\mathcal{B}^1_{(s\overline{P},c)}$ which are both tangent to $\mathcal{B}^1_{(s,c)}$. Again by Theorem 2.3, we know that starting with two such circles $\mathcal{B}^1_{(sP,c)}$ and $\mathcal{B}^1_{(s,c)}$ in $\tau(1, a^2)$ which are tangent, we end up with a proper Steiner chain. Moreover, the length of the Steiner chain is then given by the smallest integer k such that $P^k = 1$, i.e. we are back at the starting point.

Now assume that the above three conditions are satisfied. Since $-a$ is a nonsquare, we can apply Lemma 4.1 to obtain a Steiner chain. Since k is by assumption such that $P^k = 1$ but $P^l \neq 1$ for all $1 \leq l \leq k-1$, the length of the Steiner chain is indeed k. □

5 Generalization

Two disjoint circles in $\mathbb{M}(q)$ define a non-intersecting pencil. Such a pencil consist of $q-1$ circles and two limiting points. A Möbius transformation that sends the limiting points to 0 and ∞, and a point on one of the given circles to 1, will take the given circles to a pair of circles centered at 0, one of which is describes by $z\bar{z}=1$ (see [4], [5] for details, and Section 5.2). This is the same procedure as in the usual proof of Steiner's porism in the classical Möbius plane. It allows, also in $\mathbb{M}(q)$, to transform a general pair of disjoint circles into the standard pair treated in the previous sections, and to apply the corresponding results. However, it is convenient, also from a computational point of view, to skip the transformation step, and to apply the results in the previous theorems directly to a given pair of disjoint circles. This is done by introducing a Möbius invariant for arbitrary pairs of circles.

5.1 A Möbius invariant for pairs of circles

In the Euclidean plane two non-intersecting circles form a capacitor. The capacitance is a conformal invariant and therefore in particular invariant under Möbius transformations. Here we present a discrete analogue of this fact which will be used later to decide whether any two non-intersecting circles carry a Steiner chain of length k.

The *capacitance* associates an element of $\mathrm{GF}(q)$ to any pair of circles in $\mathbb{M}(q)$ and is defined as follows:

$$\begin{aligned}\mathrm{cap}(\mathcal{B}^1_{(s_1,c_1)},\mathcal{B}^1_{(s_2,c_2)}) &:= \frac{1}{c_1c_2}\big(c_1+c_2-(s_1-s_2)(\bar{s}_1-\bar{s}_2)\big)^2\\ \mathrm{cap}(\mathcal{B}^1_{(s_1,c_1)},\mathcal{B}^2_{(s_2,c_2)}) = \mathrm{cap}(\mathcal{B}^2_{(s_2,c_2)},\mathcal{B}^1_{(s_1,c_1)}) &:= \frac{1}{c_1s_2\bar{s}_2}(s_1\bar{s}_2+\bar{s}_1s_2-c_2)^2\\ \mathrm{cap}(\mathcal{B}^2_{(s_1,c_1)},\mathcal{B}^2_{(s_2,c_2)}) &:= \frac{1}{s_1\bar{s}_1s_2\bar{s}_2}(s_1\bar{s}_2+\bar{s}_1s_2)^2.\end{aligned}$$

It turns out that this quantity is indeed invariant under Möbius transformations:

Theorem 5.1. *Let $\mathcal{B}$, $\tilde{\mathcal{B}}$ be two circles and μ a Möbius transformation. Then* $\mathrm{cap}(\mathcal{B},\tilde{\mathcal{B}})=\mathrm{cap}(\mu(\mathcal{B}),\mu(\tilde{\mathcal{B}}))$.

Proof. It is easy to check that cap is invariant under translations $z\mapsto\zeta=z+a$, $a\in\mathrm{GF}(q^2)$ and similarity transformations $z\mapsto\zeta=bz$, $b\in\mathrm{GF}(q^2)\setminus\{0\}$. The only tedious part of the proof is to check that cap is invariant under the reciprocation $\mu: z\mapsto\zeta=1/z$, since in this case circles may change from first type to second type and vice versa: It is elementary to check that

$$\mu(\mathcal{B}^1_{(s,c)})=\begin{cases}\mathcal{B}^1_{\left(\frac{\bar{s}}{s\bar{s}-c},\frac{c}{(s\bar{s}-c)^2}\right)} & \text{if } s\bar{s}\neq c\\ \mathcal{B}^2_{(\bar{s},1)} & \text{if } s\bar{s}=c\end{cases}\qquad\text{and}\qquad \mu(\mathcal{B}^2_{(s,c)})=\begin{cases}\mathcal{B}^1_{\left(\frac{\bar{s}}{c},\frac{s\bar{s}}{c^2}\right)} & \text{if } c\neq 0\\ \mathcal{B}^2_{(\bar{s},0)} & \text{if } c=0.\end{cases}$$

We only carry out the invariance proof for one prototypical case of two circles $\mathcal{B}^1_{(s_1,c_1)}$ with $s_1\bar{s}_1=c_1$ and $\mathcal{B}^1_{(s_2,c_2)}$ with $s_2\bar{s}_2\neq c_2$. In this case,

$$\mathrm{cap}(\mathcal{B}^1_{(s_1,c_1)},\mathcal{B}^1_{(s_2,c_2)})=\frac{1}{c_1c_2}\big(c_1+c_2-(s_1-s_2)(\bar{s}_1-\bar{s}_2)\big)^2=\frac{1}{c_1c_2}\big(c_2+s_1\bar{s}_2+s_2(\bar{s}_1-\bar{s}_2)\big)^2 \tag{5}$$

where we have used $s_1\bar{s}_1=c_1$. On the other hand,

$$\begin{aligned}&\mathrm{cap}(\mu(\mathcal{B}^1_{(s_1,c_1)}),\mu(\mathcal{B}^1_{(s_2,c_2)}))=\mathrm{cap}\Big(\mathcal{B}^2_{(\bar{s}_1,1)},\mathcal{B}^1_{\left(\frac{\bar{s}_2}{s_2\bar{s}_2-c_2},\frac{c_2}{(s_2\bar{s}_2-c_2)^2}\right)}\Big)\\ &=\frac{1}{\frac{c_2}{(s_2\bar{s}_2-c_2)^2}s_1\bar{s}_1}\Big(\frac{\bar{s}_2}{s_2\bar{s}_2-c_2}s_1+\frac{s_2}{s_2\bar{s}_2-c_2}\bar{s}_1-1\Big)^2=\frac{(s_2\bar{s}_2-c_2)^2}{c_1c_2}\Big(\frac{\bar{s}_2}{s_2\bar{s}_2-c_2}s_1+\frac{s_2}{s_2\bar{s}_2-c_2}\bar{s}_1-1\Big)^2\end{aligned} \tag{6}$$

again since $s_1\bar{s}_1=c_1$. Obviously, the expressions in (5) and (6) agree. The other cases are similar. □

In a next step we show that, as it is the case in the classical Möbius plane, it is possible to transform any two non-intersecting Möbius circles into concentric circles.

5.2 Transformation of non-intersecting circles into concentric circles

Theorem 5.2. *Any two disjoint circles in $\mathbb{M}(q)$ can be mapped to concentric circles using a suitable Möbius transformation.*

We give a combinatorial proof which uses the following results.

Lemma 5.3. *For any given circle $\mathcal{B}$ there are $\frac{1}{2}(q^3 - 3q^2 + 2q)$ circles disjoint to $\mathcal{B}$.*

Proof. By axiom (M2), for a point P on $\mathcal{B}$ and any other point Q not on $\mathcal{B}$, there is a unique circle tangent to $\mathcal{B}$ through P and Q. There are $q^2 + 1$ points in total and $q + 1$ points on $\mathcal{B}$. So for any of the $q^2 - q$ points not on $\mathcal{B}$, there is such a unique circle through a given point P on $\mathcal{B}$. Since there are $q + 1$ points on every circle, exactly q of these tangent circles are the same. This can be done for every point on $\mathcal{B}$, which leads to $(q + 1)(q^2 - q)/q = q^2 - 1$ circles which are tangent to $\mathcal{B}$.

For the circles intersecting $\mathcal{B}$, note that by axiom (M1) there is a unique circle through two points on $\mathcal{B}$ and any other point not on $\mathcal{B}$. So for two fixed points on $\mathcal{B}$, there are $\frac{q^2-q}{q-1} = q$ circles intersecting $\mathcal{B}$ in those two points. This can be done for any pair of points on $\mathcal{B}$, which leads to $\frac{1}{2}q^2(q + 1)$ circles which intersect $\mathcal{B}$.

Since there are $q(q^2 + 1)$ circles in total, the number of circles disjoint to $\mathcal{B}$ is given by

$$q(q^2 + 1) - (q^2 - 1) - \frac{1}{2}q^2(q + 1) - 1 = \frac{1}{2}(q^3 - 3q^2 + 2q). \qquad \square$$

Lemma 5.4. *There are exactly $q^3 - q$ Möbius transformations which map the unit circle $z\overline{z} = 1$ to itself. In particular, they are given by*

$$\mu_1(z) = \frac{bz - ba}{-\overline{a}z + 1}$$

for $b\overline{b} = 1$ and $a\overline{a} \neq 1$, and by $\mu_2(z) = b/z$ for $b\overline{b} = 1$.

Proof. Recall that Möbius transformations act sharply triply transitively. So for $\{P_1, P_2, P_3\}$ on the unit circle $z\overline{z} = 1$, there are $\binom{q+1}{3}$ choices for mapping it to any three points on $z\overline{z} = 1$ again. Moreover, for any choice of three points, there are $3! = 6$ such transformations. Hence, there are $3!\binom{q+1}{3} = q^3 - q$ such Möbius transformations.

Let us have a closer look at μ_1. Of course, we have

$$\left(\frac{bz - ba}{-\overline{a}z + 1}\right)\overline{\left(\frac{bz - ba}{-\overline{a}z + 1}\right)} = 1$$

whenever $b\overline{b} = 1$ and $z\overline{z} = 1$. The condition $a\overline{a} \neq 1$ ensures that we do not divide by 0. There are $q+1$ choices for b and $q^2 - (q + 1)$ choices for a. Hence there are $q^3 - 2q - 1$ transformations μ_1.

Similarly, μ_2 maps the unit circle to itself whenever $b\overline{b} = 1$, so there are $q+1$ such transformations. Since $(q^3 - 2q - 1) + (q + 1) = q^3 - q$, these are indeed all such transformations. $\square$

Now we are ready to prove Theorem 5.2.

Proof of Theorem 5.2. There are $q - 2$ circles concentric to $z\overline{z} = 1$, namely all those circles $z\overline{z} = c$ for $c = 2, \ldots, q - 1$. We now apply all the Möbius transformations, which map the unit circle to itself, to those concentric circles.

Note that every image occurs exactly $2(q + 1)$ times. To see this, consider first the circle $z\overline{z} = c$ for $c \in \{2, \ldots, q - 1\}$ fixed. Clearly, μ_1 for choosing $a = 0$ maps $z\overline{z} = c$ to $z\overline{z} = c$, for all $b\overline{b} = 1$. Moreover, applying μ_2 to $z\overline{z} = \frac{1}{c}$ gives $z\overline{z} = c$ as well, for all $b\overline{b} = 1$. Since for any other choice of a in μ_1, the center of $z\overline{z} = c$ is translated, the circle $z\overline{z} = c$ occurs $2(q + 1)$ times when applying all $q^3 - q$ Möbius transformations μ_1 and μ_2 described above to $z\overline{z} = c$. Similarly we can be proceed for other circles $(z - s)(\overline{z} - \overline{s}) = c$.

So we apply the $q^3 - q$ Möbius transformations to the $q - 2$ circles concentric to $z\overline{z} = 1$. Every image occurs $2(q + 1)$ times, i.e. we get

$$\frac{(q - 2)(q^3 - q)}{2(q + 1)} = \frac{1}{2}(q^3 - 3q^2 + 2q)$$

circles, which is by Lemma 5.3 exactly the number of circles disjoint to $z\overline{z} = 1$. $\square$

5.3 General criterion for Steiner chains

Let $\mathcal{B}$ and $\tilde{\mathcal{B}}$ be non-intersecting circles in $\mathbb{M}(q)$. As we have seen in Section 5.2, it is possible to transform them into $\mu(\mathcal{B}) = \mathcal{B}^1_{(0,1)}$, $\mu(\tilde{\mathcal{B}}) = \mathcal{B}^1_{(0,b)}$ by a suitable Möbius transformation. By Theorem 5.1 we have

$$\kappa := \operatorname{cap}(\mathcal{B}, \tilde{\mathcal{B}}) = \operatorname{cap}(\mu(\mathcal{B}), \mu(\tilde{\mathcal{B}})) = \operatorname{cap}(\mathcal{B}^1_{(0,1)}, \mathcal{B}^1_{(0,b)}) = \frac{1}{b}(1+b)^2.$$

Solving for b gives $b = \frac{1}{2}(\kappa - 2 \pm \sqrt{\kappa(\kappa-4)})$. Changing between the two possible signs corresponds to applying an additional inversion $z \mapsto 1/z$ to both circles, and we may take the plus sign by convention. Then the general criterion follows from Theorem 4.8:

Theorem 5.5. *Let $\mathcal{B}$ and $\tilde{\mathcal{B}}$ be non-intersecting circles, let $\kappa := \operatorname{cap}(\mathcal{B}, \tilde{\mathcal{B}})$ and $b := \frac{1}{2}(\kappa - 2 + \sqrt{\kappa(\kappa-4)})$, and let $b = a^2$ with a in $\mathrm{GF}(q)$. Then $\mathcal{B}$ and $\tilde{\mathcal{B}}$ carry a Steiner chain of length $k \geq 3$ if and only if the following conditions are satisfied:*

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

(2) *a solves the equation $P^k = 1$ where P is given by*

$$P = \frac{-a^2 + 6a - 1 + 4(a-1)\sqrt{-a}}{(1+a)^2} \tag{7}$$

but $P^l \neq 1$ for $1 \leq l \leq k-1$.

6 Comparison to the Euclidean plane

Steiner's Porism is well understood in the Euclidean plane. For two concentric circles of radius 1 and R, a Steiner chain of length k which wraps around the inner circle once can be constructed if and only if

$$R = \frac{1+\sin(\varphi)}{1-\sin(\varphi)}$$

where $\varphi = \frac{\pi}{k}$. For some values of k, we can express $\sin(\frac{\pi}{k})$ explicitly in terms of radicals. In the following table, we calculate R for some values of k.

k	$\frac{180}{k}$	$\sin\frac{\pi}{k}$	R
3	60	$\frac{\sqrt{3}}{2}$	$7+4\sqrt{3}$
4	45	$\frac{\sqrt{2}}{2}$	$3+2\sqrt{2}$
5	36	$\frac{\sqrt{10-2\sqrt{5}}}{4}$	$11-4\sqrt{5}+2\sqrt{50-22\sqrt{5}}$
6	30	$\frac{1}{2}$	3
8	22.5	$\frac{\sqrt{2-\sqrt{2}}}{2}$	$7-4\sqrt{2}+2\sqrt{20-14\sqrt{2}}$

Table 1: Some values for Steiner chains of length k.

Note that our values for R coincide with the values for a calculated in the Lemmas 4.3, 4.4, 4.6, 4.5 and 4.7. Let us have a closer look at why this is the case. Recall that for two common tangent circles of $\mathcal{B}_1$ and $\mathcal{B}_{a^2}$, we calculated in Lemma 4.1 the point in which the second circle of the chain is tangent to $\mathcal{B}_1$, namely

$$P = \frac{-a^2 + 6a - 1 + 4(a-1)\sqrt{-a}}{(1+a)^2}. \tag{8}$$

For the construction of a Steiner chain, we needed $-a$ to be a nonsquare in $\mathrm{GF}(q)$. So we rewrite P as

$$P = \frac{-a^2 + 6a - 1}{(1+a)^2} + \sqrt{-a}\frac{4(a-1)}{(1+a)^2}. \tag{9}$$

Note that $\frac{-a^2+6a-1}{(1+a)^2}$ and $\frac{4(a-1)}{(1+a)^2}$ are both in $\mathrm{GF}(q)$. By assumption, $\sqrt{-a}$ is not in $\mathrm{GF}(q)$, so we consider P as an element of $\mathrm{GF}(q)(\sqrt{-a})$, which is isomorphic to $\mathrm{GF}(q^2)$. So we can write all elements of $\mathrm{GF}(q)(\sqrt{-a})$ in the form $z = x + y\sqrt{-a}$. We refer to x as the *real part* of z, denoted by $\Re(z)$, and to y as the *imaginary part* of z, denoted by $\Im(z)$.

Recall that for a Steiner chain of length k the tangent points on $\mathcal{B}_1$ are given by $1, P, P^2, \ldots, P^{k-1}$. The real part of P^2 satisfies

$$\Re(P^2) = 2\Re(P)^2 - 1$$

and the imaginary part of P satisfies

$$\Im(P^2) = 2\Re(P)\Im(P).$$

Note that those equations are the same as for the sine and cosine in the Euclidean plane, namely $\cos(2\varphi) = 2\cos(\varphi)^2 - 1$ and $\sin(2\varphi) = 2\cos(\varphi)\sin(\varphi)$. Hence calculating P^2 is in a sense the same as doubling the angle between 1 and P.

Acknowledgements: We would like to thank J. Chris Fisher for his very helpful comments and detailed suggestions which helped to improve the presentation of this article considerably.

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*. Reprint of the 1916 edition. 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, Automorphismen endlicher Möbius-Ebenen. *Math. Z.* **87** (1965), 115–136. MR0177345 Zbl 0132.14303
[5] P. Dembowski, *Finite geometries*. Springer 1997. MR1434062 Zbl 0865.51004
[6] G. H. Hardy, E. M. Wright, *An introduction to the theory of numbers*. Oxford Univ. Press 2008. MR2445243 Zbl 1159.11001
[7] R. Lidl, H. Niederreiter, *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge Univ. Press 1997. MR1429394 Zbl 0866.11069
[8] D. Pedoe, *Geometry*. Dover Publications, New York 1988. MR1017034 Zbl 0716.51002
[9] P. Yiu, Rational Steiner porism. *Forum Geom.* **11** (2011), 237–249. MR2877262 Zbl 1287.51002
[10] H. Zeitler, "Touching-cycle-chains" in finite Miquelian Möbius planes. In: *Proceedings of the conference on combinatorial and incidence geometry: principles and applications* (*La Mendola,* 1982), volume 7 of *Rend. Sem. Mat. Brescia*, 645–656, Vita e Pensiero, Milan 1984. MR758854 Zbl 0559.51006