Links among Finite Geometries, Graphs and Groups

Ph.D. dissertation

János Ruff

Supervisor: György Kiss, Ph.D.

Doctoral School in Mathematics and Computer Science
University of Szeged
Bolyai Institute

2010

Contents

Acknowledgements

This dissertation could not be possible without the encouragement and support of many people at different times and places. I can not thank to everyone individually but I would like to express my gratitude to all of them.

First of all I wish to express my deepest gratitude to my advisor György Kiss for teaching me the beauty of finite geometry and for giving me the topics for dissertation and for the invaluable help in my work. I also thank for providing me a lot of possibilities.

I am also thankful to my coauthors for all their help and teaching. Special thanks are due to István Kovács for his friendship and everlasting belief in me.

I would like to thank to all my collegues at the Institute of Mathematics and Informatics at the University of Pécs for providing me a friendly environment for my work.

And last but not least I am indebted to my wife, parents and friends for their unerring support and for always being there for me.

Chapter 1

Semiovals contained in the union of three non-concurrent lines

1.1 Introduction

In this chapter we summarize some results on semi quadratic sets and semiovoids, and later we discuss the properties of semiovals contained in three non-concurrent lines. Semiovals first appeared as special examples of *semi-quadratic sets.* Let Π be a projective space and $\mathcal{Q} = (\mathcal{P}, \mathcal{L})$ be a pair consisting of a set $\mathcal{P}$ of points of Π, and a set $\mathcal{L}$ of lines of Π. A *tangent* to $\mathcal{Q}$ at $P \in \mathcal{P}$ is a line $\ell \in \mathcal{L}$ such that P is on ℓ, and either $\ell \cap \mathcal{P} = \{P\}$, or $\ell \in \mathcal{L}$. $\mathcal{Q}$ is called a *semi quadratic set* (SQS), if every point on a line of $\mathcal{L}$ belongs to $\mathcal{P}$, and for all $P \in \mathcal{P}$ the union $\mathcal{T}_P$ of all tangents to $\mathcal{Q}$ at P is either a hyperplane or the whole space Π. A lot of attempts were made to classify all SQS, but the problem is still open in general. For the known results about SQS we refer to [12] and [29].

An SQS $\mathcal{Q} = (\mathcal{P}, \mathcal{L})$ is called a *semi-ovoid* (or *semioval* if $\dim \Pi = 2$), if $\mathcal{L} = \emptyset$ and $\mathcal{P}$ contains at least 2 points. The complete characterization of semi-ovoids was given by J. Thas [46]. Using elementary double counting arguments, he proved the following results.

Theorem 1.1.1.

- *The only semi-ovoids of $PG(3, q)$ are the ovoids (set of $q^2 + 1$ points, no three of them are collinear).*
- *In $PG(n, q)$, $n > 3$, there are no semi-ovoids.*

In the planar case the situation is much more complicated. It is easy to see, that the following simpler definition of semiovals is equivalent to the previously given one.

Definition 1.1.2. *Let Π be a projective plane of order q. A semioval in Π is a non-empty pointset S with the property that for every point P in S there exists a unique line t_P such that $S \cap t_P = \{P\}$. This line is called the tangent to S at P.*

The classical examples of semiovals arise from polarities (ovals and unitals), and from the theory of blocking sets (the vertexless triangle). The study of semiovals is motivated by their applications to cryptography [4], too.

It is known that $q+1 \leq |S| \leq q\sqrt{q}+1$ and both bounds are sharp [46], [28].

For planes of small order the complete spectrum of the sizes and the number of projectively non-isomorphic semiovals are known. For $q = 2$ and $q = 3$ we give the complete description:

$q = 2$: Because of the bounds on the cardinality, each semioval consists of three points, and these points are not collinear, hence semiovals are ovals.

$q = 3$: If a semioval S is not an oval, then there is a line ℓ which contains three points of S, say A, B and C. There are four lines through each of these points, one of them is the tangent, but the others must meet S. Hence S contains at least two points not on ℓ. Let $D, E \in S \setminus \ell$. If F is the fourth point of the line ℓ, then $t_D \cap \ell = t_E \cap \ell = F$, thus $DE \cap \ell \neq F$. Without loss of generality we may assume, that $DE \cap \ell = A$. This implies that S must contain a sixth point G, otherwise there would be two tangents through A. But 6 is an upper bound of the cardinality of S by Theorem 1.1.1. If $G = BD \cap CE$, then it is easy to check that the set $\{A, B, C, D, E, G\}$ is a semioval. These points form the vertices of a complete quadrilateral. Hence we proved that there are two projectively non-isomorphic classes of semiovals in $\mathrm{PG}(2, 3)$.

From now on in the rest of the chapter we suppose that $q > 3$.

Because of the huge diversity of semiovals, the complete classification is hopeless. To reduce the number possibilities we will assume some extra properties.

A semioval is said to be *regular with character a* if all nontangent lines intersect S in either 0 or a points. Regular semiovals were studied by Blokhuis and Szőnyi [10], and Gács [22], who proved that in $PG(2, q)$ each regular semioval is either an oval or a unital.

Semiovals with large collinear subsets were investigated by Dover [20]. He proved the following properties of the semioval S:

- $|S \cap \ell| \leq q - 1$ for any line ℓ of Π.

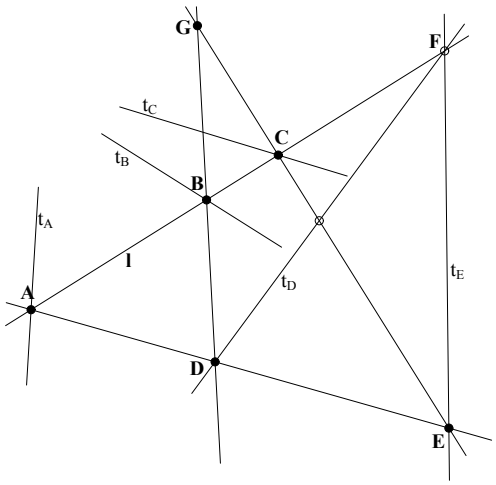

Figure 1.1: The $q = 3$ case

- If S has a $(q-1)$-secant, then $2q - 2 \leq |S| \leq 3q - 3$.
- If S has more than one $(q-1)$-secant, then S can be obtained from a vertexless triangle by removing some subset of points from one side.

It is trivial that a line ℓ, or any proper subset of ℓ is not a semioval, because the number of tangent lines at each of its point is greater than 1. A semioval S could not contain a whole line ℓ, because if $P \in S \setminus \ell$, then any line through P meets ℓ, hence there is no tangent to S at P. In $\mathrm{PG}(2,2)$ and $\mathrm{PG}(2,3)$ there are semiovals containing q (that is 2 or 3, respectively) collinear points. But for $q > 3$ the size of the largest collinear subset in a semioval is at most $q - 1$, we give a different proof from the original one due to Dover.

Theorem 1.1.3. *Let S be a semioval in Π_q, $q > 3$. Then for any line ℓ the intersection $S \cap \ell$ contains at most $q - 1$ points.*

Proof. Suppose that $|S \cap \ell| = q$. Then there is a unique point $T \in \ell \setminus S$. If $P \in S \setminus \ell$, then t_P must meet ℓ in T. Hence $|S \setminus \ell| \leq q$, because the tangents at distinct points are distinct lines, there are $q + 1$ lines through T, but one of them, ℓ, could not be a tangent line. On the other hand, if $R \in \ell \setminus \{T\}$, then there are $q + 1$ lines through R, one of them is ℓ, one of them is t_R, but each of the remaining $q - 1$ contains at least one point of $S \setminus \ell$, thus $|S \setminus \ell| \geq q - 1$.

Suppose that $|S \setminus \ell| = q - 1$, and let P_1 and P_2 be two distinct points in $S \setminus \ell$ (they exist because $q > 3$). If $P_1P_2 \cap \ell = T$, then there is no tangent

line to S at P_1 (and at P_2). If $P_1P_2 \cap \ell = R \neq T$, then there are more than one tangent lines at R, both of these are contradictions.

If $|S \setminus \ell| = q$, then let $S \setminus \ell = \{P_1, P_2, \ldots, P_q\}$. Now no line of type P_iP_j meets ℓ in T, because we have already seen, that $t_{P_i} = P_iT$. Consider the $q(q-1)/2$ pairs of points $\{P_i, P_j\}$ for all $i \neq j$. Each pair corresponds to a line P_iP_j. Suppose, that $\{P_i, P_j\} \neq \{P_k, P_l\}$ and $P_iP_j \cap P_kP_l = R \in \ell \setminus \{T\}$. Then there would be more than one tangent line at R, hence the lines corresponding to distinct pairs meet $\ell \setminus \{T\}$ in distinct points. This implies

$$\frac{q(q-1)}{2} \leq q, \quad \text{so} \quad q \leq 3.$$

This contradiction finishes the proof. ■

There are several results about sets which are contained in the union of three lines and have some other properties. For example Cameron [13] and Szőnyi [45] gave complete description of minimal blocking sets of this type.

The aim of the first two chapters is to characterize the semiovals which are contained in the union of at most three lines. We will use the following notation throughout this chapter: Π is a projective plane of order q, S is a semioval in Π, if Q is a point of S then t_Q is the unique tangent to S at Q, $\mathcal{P}_Q$ is the pencil of lines with carrier Q, ℓ_1, ℓ_2 and ℓ_3 are the three lines whose union contains S, $L_i = S \cap \ell_i$ for $i = 1, 2, 3$, and $P_i = \ell_k \cap \ell_j$ where $\{i, j, k\} = \{1, 2, 3\}$.

1.2 Preliminaries

It follows from the definition that a semioval could not be contained in one line. Suppose now that S is contained in the union of two lines, ℓ_1 and ℓ_2. Among the elements of $\mathcal{P}_{P_3}$ there exist $(q+1) - 2 = q - 1$ lines which are tangent to S at P_3, so if $q > 2$ then $P_3 \notin S$. Let us choose an arbitrary point $Q \in L_1$. Then $q - 1$ out of the q lines of $\mathcal{P}_Q \setminus \ell_1$ must intersect ℓ_2 hence $|L_2| = q - 1$, and because of the symmetry $|L_1| = q - 1$. If $Q_i \in \ell_i$ are arbitrary points $(i = 1, 2)$, then the pointset $\ell_1 \cup \ell_2 \setminus \{P, Q_1, Q_2\}$ is a semioval, because for each $R_i \in S$ the unique tangent t_{R_i} is the line R_iQ_j where $\{i, j\} = \{1, 2\}$. Hence we proved the following:

Proposition 1.2.1. *Let S be a semioval in a projective plane of order $q > 2$. If S is contained in the union of two lines ℓ_1 and ℓ_2, then $|S| = 2(q-1)$ and $S = \ell_1 \cup \ell_2 \setminus \{\ell_1 \cap \ell_2, Q_1, Q_2\}$ where $Q_i \in \ell_i$ for $i = 1, 2$.* ■

If S is contained in the union of three lines, then there are much better bounds on the size of S than the general ones.

Proposition 1.2.2. *Let S be a semioval in a projective plane Π of order q. If S is contained in the union of three lines then*

$$\frac{3(q-1)}{2} \leq |S| \leq 3(q-1).$$

Proof. We may assume that $q > 4$ because if $q \leq 4$, then the bounds of Hubaut are sharper than the bounds of our proposition. The upper bound is a trivial consequence of 1.1.3.

In the case of the lower bound we distinguish two possibilities. If ℓ_1, ℓ_2 and ℓ_3 are concurrent, then their point of intersection $P_1 (= P_2 = P_3)$ does not belong to S, because $P_1 \in S$ would imply that there were $(q+1)-3 > 2$ tangents to S at P_1. Let now $Q \in L_i$ be any point of S. Among the $q+1$ lines of $\mathcal{P}_Q$ there are two exeptional ones, t_Q and ℓ_i, each of the remaining $q-1$ lines meets either L_j or L_k where $\{i,j,k\} = \{1,2,3\}$. Thus $|L_j| + |L_k| \geq q-1$. This holds for all the three possible pairs (j,k), hence $|L_1| + |L_2| + |L_3| \geq 3(q-1)/2$.

If ℓ_1, ℓ_2 and ℓ_3 form a triangle, and $P_i \notin S$ then the same argument shows that $|L_j| + |L_k| \geq q-1$. If $P_i \in S$ then $|L_i| \geq q-2$, because among the lines of $\mathcal{P}_{P_i}$ there is only one, t_{P_i}, which does not contain some other points of S. Let $Q \in L_i$ be an arbitrary point. Now we get $|L_j| + |L_k| \geq q-2$. Hence in both cases $|L_i| + |L_j| + |L_k| \geq 3(q-1)/2$. ■

1.3 Semiovals contained in the sides of a triangle

In the rest of the chapter semiovals in $PG(2,q)$ which are contained in the union of three lines are studied. We assume that S is not contained in the union of two lines, thus $L_i \setminus \{P_j, P_k\} \neq \emptyset$ for $\{i,j,k\} = \{1,2,3\}$. In Section 1.3 a complete classification is given when the lines form a triangle. We prove that each semioval belongs to one of the following three classes.

1. S has a $(q-2)$-secant and two $(t+1)$-secants for a suitable t. A semioval in this class exists if and only if $q = 4$ and $t = 1$, $q = 8$ and $t = 4$ or $q = 32$ and $t = 26$.

2. S has two $(q-1)$-secants and a k-secant. Semiovals in this class exist for all $1 < k < q$.

3. S has three $(q-1-d)$-secants. Semiovals in this class exist if and only if $d|(q-1)$.

Proposition 1.3.1. *S contains at most one point from the set $\{P_1, P_2, P_3\}$.*

Proof. If $P_i \in S$ then $|L_i \setminus \{P_j, P_k\}| = q-2$. Thus $\{P_1, P_2, P_3\} \subset S$ implies $|L_i| = q$, contradicting to the previously cited theorem of Dover. Suppose now that $P_1, P_2 \in S$ and $P_3 \notin S$. Then $|L_1| = |L_2| = q-1$. Let E_i $(i = 1, 2)$ be the unique point of ℓ_i which is not in L_i and different from P_3. For each $A \in L_1$ t_A must be the line AE_2, hence $AE_2 \cap \ell_3 \notin S$, so L_3 contains exactly three points: P_1, P_2 and $E_1E_2 \cap \ell_3 = E_3$. But at E_3 there are two distinct tangents to S, the lines E_3P_3 and E_3E_1. This contradiction proves the statement. ■

Theorem 1.3.2. *A semioval in $PG(2,q)$ which is contained in the sides of a triangle and which contains one vertex of this triangle has a $(q-2)$-secant and two $(t+1)$-secants where t is a suitable integer. This type of semiovals exists if and only if $q = 4$ and $t = 1$, $q = 8$ and $t = 4$ or $q = 32$ and $t = 26$.*

Proof. If S contains P_3 then Proposition 2.1 implies that neither P_1 nor P_2 are in S and $|L_3| = q-2$. Hence there exists a point Q such that $\ell_3 \setminus L_3 = \{P_2, P_3, Q\}$. Let us choose the system of reference such that

$$P_1 = (1,0,0),\ P_2 = (0,1,0),\ P_3 = (0,0,1),\ Q = (1,1,0).$$

Let

$$A_1 = \{a \in GF^*(q) :\ (a,0,1) \in S\}$$

and

$$A_2 = \{a \in GF^*(q) :\ (0,-a,1) \in S\}.$$

First we show that $A_1 = A_2$. If $R \in L_i$ is an arbitrary point $(i = 1, 2)$ then t_R is the line RP_i hence RQ contains at least two – and so exactly two – points of S. But the points $Q = (1,1,0)$, $(a,0,1)$ and $(0,-a,1)$ are collinear. Thus $(a,0,1) \in S$ if and only if $(0,-a,1) \in S$. Let now $t = |A_1| = |A_2|$.

If $1 \neq m \in GF^*(q)$ then $M = (m,1,0) \in L_3 \subset S$. Consider the elements of $\mathcal{P}_M$. The line ℓ_3 is a $(q-2)$-secant of S, t_M is a tangent, each of the remaining $q-1$ lines is either a 2-secant or a 3-secant of S. Each 2-secant contains one point of $L_1 \cup L_2$ while each 3-secant contains one point of L_1 and one point of L_2. The cardinality of $L_1 \cup L_2$ is $2t+1$, so if the number of 3-secants is λ, then $2\lambda + (q-1-\lambda) = 2t+1$. Hence there are exactly $\lambda = 2t+2-q$ 3-secants of S in $\mathcal{P}_M$.

A 3-secant contains the points $(b,0,1)$, $(0,-c,1)$ and $(m,1,0)$ if and only if $m = c/b$. Hence S is a semioval if and only if for all $1 \neq m \in GF^*(q)$ there exist exactly $\lambda = 2t+2-q$ pairs of elements (b,c) of $A_1 \times A_1$ for which $m = c/b$ hold. This means that A_1 is a difference set in $GF^*(q)$ with parameters $v = q-1, k = t, \lambda = 2t+2-q$. For the basic facts about difference sets we refer to the survey of Baumert [5] .

If a (v, k, λ)-difference set exists, then its parameters satisfy the equation $k(k-1) = (v-1)\lambda$, hence in our case

$$t(t-1) = (q-2)(2t+2-q).$$

Solving this equation and using $t < q$ we get the parameters of the difference set:

$$v = q-1,\ k = q - \frac{3+\sqrt{4q-7}}{2},\ \lambda = q-1-\sqrt{4q-7}.$$

Thus if $n = k - \lambda$ then

$$n^2+n+1 = \frac{4q-7-2\sqrt{4q-7}+1}{4} + \frac{\sqrt{4q-7}-1}{2} + 1 = q-1,$$

so the difference set is a planar one.

If q is odd then $4q-7 \equiv 5 \pmod 8$, hence $4q-7$ is not a square. Thus this type of difference set does not exist for q odd. So semiovals belonging to this class could exist only for q even. If q is even then $4q-7$ is a square if and only if $4q = 2^r$ and the diophantine equation $2^r = x^2+7$ has a solution. This equation was solved by Nagell [40]. He proved that there are five solutions, namely the pairs $(r, x) = (3, 1)$, $(4, 3)$, $(5, 8)$, $(7, 11)$, and $(15, 181)$.

If $r = 3$ then $q = 2$, contrary to our assumption $q > 2$. If $r = 4$ then $q = 4$ and $\lambda = 0$, so there is no three-secant, the semioval contains five points, it is an oval. If $r = 5$ then $q = 8$ and the difference set has parameters $v = 7$, $k = 4$ and $\lambda = 2$. A difference set with these parameters exists, this is the complementary difference set of the well-known $(7, 3, 1)$-difference set belonging to the Fano plane. The corresponding semioval in $PG(2, 8)$ consists of 15 points, it has two 5-secants and one 6-secant. If $r = 7$ then $q = 32$ and the difference set has parameters $v = 31$, $k = 25$ and $\lambda = 20$. Such difference set exists, this is the complementary difference set of the $(31, 6, 1)$-difference set which belongs to the projective plane of order $q = 5$. Hence the semioval appears in $PG(2, 32)$. It has 81 points, two 26-secants and one 30-secant. If $r = 13$ then $q = 8192$ and the parameters are $v = 8191$, $k = 181$, $\lambda = 91$ and $n = 90$. There is no planar difference set with these parameters, because it is known (see [24]) that for $n < 2,000,000$ the order of each cyclic projective plane is a prime power. ■

Now consider the cases when S does not contain any point from the set $\{P_1, P_2, P_3\}$. The vertexless triangle T is a semioval belonging to this class. Let D be any set of points on one side of T. If $0 < |D| < q-2$, then it is easy to show that the set $T \setminus D$ is a semioval. These semiovals form Class 2. If we delete points from more than one side of T, then the semioval belongs to Class 3.

Theorem 1.3.3. *If a semioval S in $PG(2,q)$ is contained in the sides of a triangle T, does not contain any vertex of T and has at most one $(q-1)$-secant, then S has exactly three $(q-1-d)$-secants where d is a suitable divisor of $q-1$.*

Proof. Let us choose the system of reference such that the lines ℓ_1 and ℓ_2 are not $(q-1)$-secants. Then we may assume that $P_1=(1,0,0), P_2=(0,1,0), P_3=(0,0,1)$, and the points $(1,0,1)$ and $(0,1,1)$ are not in S. Let

$$A=\{a\in GF^*(q):\ (a,0,1)\notin S\},$$

$$B=\{b\in GF^*(q):\ (0,b,1)\notin S\}$$

and

$$C=\{c\in GF^*(q):\ (-c,1,0)\notin S\}.$$

We prove that $A=B=C$. If $Q_i\in L_i$ then t_{Q_i} is the line Q_iP_i for $i=1,2,3$. Thus if two points, U and V from two distinct sides of T are not in S, W denotes the point of intersection of the line UV and the third side of T, then W could not be in S because the line UV would be another tangent through W. The points $(a,0,1)$, $(0,b,1)$ and $(c,1,0)$ are collinear if and only if $a=bc$. Hence $a\in A$ and $b\in B$ imply $a/b\in C$, $a\in A$ and $c\in C$ imply $a/c\in B$, and $c\in C$ and $b\in B$ imply $bc\in A$. So $1\in C$, because $1\in A\cap B$. But this means that $A\subset B$ and $B\subset A$, hence $A=B$. In the same way we get $A=C$. Hence $a\in A$ and $b\in A$ imply $ab\in A$, and $1\in A$ and $a\in A$ imply $1/a\in A$. This means that A is a subgroup of $GF^*(q)$.

If $G\neq GF^*(q)$ is an arbitrary subgroup, then the pointset

$$\{(h,0,1),(0,h,1),(-h,1,0)\ :h\in GF^*(q)\setminus G\}$$

is a semioval with cardinality $3(q-1-|G|)$, because the lines with equation $X_1=hX_3$, $X_2=hX_3$, $X_1=-hX_2$ are the unique tangent lines at the points $(h,0,1)$, $(0,h,1)$, $(-h,1,0)$, respectively. ■

1.4 A possible generalization

A generalization to the concept of semiovals, namely semiarcs were studied by B. Csajbók and Gy. Kiss in [15]. Semiarcs are the natural generalizations of arcs. Let Π_q be a projective plane of order q. A non-empty pointset $\mathcal{S}_t\subset\Pi_q$ is called a *t-semiarc* if for every point $P\in\mathcal{S}_t$ there exist exactly t lines $\ell_1,\ell_2,\dots\ell_t$ such that $\mathcal{S}_t\cap\ell_i=\{P\}$ for $i=1,2,\dots,t$. These lines are called the tangents to $\mathcal{S}_t$ at P. If a line ℓ meets $\mathcal{S}_t$ in $1<k$ points, then ℓ is called a k-secant of $\mathcal{S}_t$. If $t=1$ examples for semiarcs are the semiovals.

In [15] similar results are proved for semiarcs.

The following lower bound on the cardinality of t-semiarcs is trivial consequence of the definition.

Proposition 1.4.1. *If $\mathcal{S}_t$ is a t-semiarc in Π_q, then $q - t + 2 \leq |\mathcal{S}_t|$.*

This bound is sharp, because any $(q - t + 2)$-arc in Π_q is a t-semiarc.

For the cardinality the following upper bound holds:

Theorem 1.4.2. *If $\mathcal{S}_t$ is a t-semiarc in Π_q, then*

$$|\mathcal{S}_t| \leq 1 + \left\lfloor \frac{q(t - 1 + \sqrt{4tq - 3t^2 + 2t + 1})}{2t} \right\rfloor .$$

They also proved better bounds for semiarcs with long secants. For the case when the semiarc is contained in 3 lines and not contained in any two lines we will refer later in Chapter 2.

Chapter 2

Semiovals contained in the union of three concurrent lines

2.1 Introduction

The aim of this chapter is to investigate semiovals which are contained in the union of three concurrent lines but are not contained in the union of any two of these lines. In the previous chapter we discussed the case when the semioval is contained in two lines.

There are only two known examples of this type. First, an infinite family arising from Baer subplanes of $\mathrm{PG}(2,q)$, where q is an even power of a prime [32]; a detailed description is given in Example 2.2.3. And second, a sporadic example in $\mathrm{PG}(2,5)$, where $\mathcal{S}$ is an irreducible conic and the intersection of the three lines is any inner point of it.

The semiovals of the above infinite family have an additional property defined below. To this end let us first introduce some standard terminology and notation, to be used throughout the rest of this chapter. For a point Q of a semioval $\mathcal{S}$ in a projective plane Π_q of order q, we let t_Q be the unique tangent to $\mathcal{S}$ at Q, and $\mathcal{P}_Q$ the pencil of lines with carrier Q. Further, we let ℓ_1, ℓ_2 and ℓ_3 be the three concurrent lines whose union contains $\mathcal{S}$, we denote by C the common point of these three lines and by $\mathcal{L}$ the union of ℓ_1, ℓ_2 and ℓ_3. And finally, we let $\mathcal{L}_i = \mathcal{S} \cap \ell_i$ $(i = 1, 2, 3)$. Now, a semioval $\mathcal{S}$ is *strong* if, for any point $K \in \mathcal{L} \setminus (\mathcal{S} \cup \{C\})$, the number of two-secants of $\mathcal{S}$ passing through K is independent of K.

In Section 2.2 we give an improved upper bound for the size of semiovals in Π_q (see Theorem 2.2.2), and show that this bound is sharp (see Example 2.2.3). In Section 2.3 we give an algebraic description of semiovals in $\mathrm{PG}(2,q)$. Finally, Section 2.4 is devoted to the study of strong semiovals.

We present some necessary conditions for the existence of such objects and give a complete classification of strong semiovals in $\mathrm{PG}(2,p)$ and $\mathrm{PG}(2,p^2)$, p an odd prime.

2.2 Bounds on the size of $\mathcal{S}$

The following lower bound for the cardinality of $\mathcal{S}$ was proved in the previous chapter.

Theorem 2.2.1. *If a semioval $\mathcal{S}$ in $PG(2,q)$, $q > 9$, is contained in the union of three concurrent lines, then $|\mathcal{S}| > 3(q-1)/2$.*

On the other hand, the best known upper bound for the size of $\mathcal{S}$ is $3(q-1)$. This follows from a result of Dover which says that a semioval in Π_q cannot contain more than $q-1$ collinear points [20]. In Theorem 2.2.2 below we improve this bound. As shown in Example 2.2.3, the bound is sharp.

Theorem 2.2.2. *If a semioval $\mathcal{S}$ in Π_q, $q > 3$, is contained in the union of three concurrent lines, then $|\mathcal{S}| \leq 3\lceil q - \sqrt{q} \rceil$.*

Proof. Let $a_i = |\mathcal{L}_i|$ for $i = 1, 2, 3$. First we prove that $a_1 = a_2 = a_3$. Let $P_1 \in \mathcal{L}_1$ be an arbitrary point. Let s_2 and s_3 be the number of lines of $\mathcal{P}_{P_1}$ meeting $\mathcal{S}$ in two and three points, respectively. Then $s_2 + s_3 = q - 1$ and $s_2 + 2s_3 = a_2 + a_3$, and hence

$$s_3 = a_2 + a_3 - (q-1).$$

This means that the total number of lines meeting $\mathcal{S}$ in three points equals

$$a_1 a_2 + a_1 a_3 - (q-1)a_1.$$

If we count the three-secants of $\mathcal{S}$ in the same way, but starting from a point $P_2 \in \mathcal{L}_2$ or a point $P_3 \in \mathcal{L}_3$, then we get that the total number of the three-secants equals

$$a_2 a_1 + a_2 a_3 - (q-1)a_2$$

and

$$a_3 a_1 + a_3 a_2 - (q-1)a_3,$$

respectively. Using these three expressions for the total number of lines meeting $\mathcal{S}$ in three points, we have that for $\{i,j,k\} = \{1,2,3\}$ pairwise distinct,

$$(a_i - a_j)\big(a_k - (q-1)\big) = 0. \tag{2.1}$$

If $q > 3$ and $\mathcal{S}$ is not contained in the union of two lines, then $C \notin \mathcal{S}$, because otherwise there would be at least 2 tangent lines through C. With the assumption $C \notin \mathcal{S}$, we prove that $a_k - (q-1) \neq 0$. For this let us suppose that $a_1 = q - 1$. This implies that there exists a unique point M on ℓ_1 different from C not in $\mathcal{L}_1$. If we choose an arbitrary point N from $\mathcal{L}_2$ the unique tangent line through N should be the line determined by the points N and M. The intersection of this line and ℓ_3 can not be in $\mathcal{S}$. If we choose N_1 from $\mathcal{L}_2$ different from N the line MN_1 will intersect ℓ_3 again in $\mathcal{S} \setminus \mathcal{L}_3$. If these N's run over the set $\mathcal{L}_2$ we get $q - a_3 \geq a_2$ (see Figure 2.1). On the other hand from the previous calculations it is obvious that $a_2 + a_3 \geq q-1$. Hence $a_2 + a_3$ can only be q or $q-1$. This shows that for any $P \in \mathcal{L}_1$ the value of s_3 is 0 or 1 which means that the total number of three secants (which is $a_2 a_3$ now) is at most $q - 1$. With these two conditions for a_2 and a_3 we deduce that one of them is 1 which leads to contradiction because through this point in $\mathcal{L}_2$ (or symmetrically in $\mathcal{L}_3$) there would be 2 tangents.

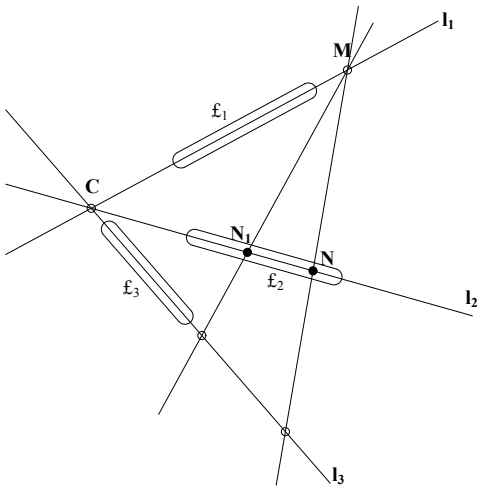

Figure 2.1: $q - a_3 \geq a_2$

Thus, (2.1) implies $a_1 = a_2 = a_3$. Let us denote this number by a. Then $|\ell_i \setminus (\mathcal{L}_i \cup \{C\})| = q - a$ for $i = 1, 2, 3$. So there are at most $(q-a)^2$ tangent lines to $\mathcal{S}$ at the points of $\mathcal{L}_i$. Hence $(q-a)^2 \geq a$, and thus $q \geq a + \sqrt{a}$. From this inequality we get

$$\sqrt{a} \leq \frac{-1 + \sqrt{1+4q}}{2} < \sqrt{q - \sqrt{q} + 1}.$$

Hence

$$a \leq \lceil q - \sqrt{q} \rceil.$$

■

This bound is sharp as the following example shows.

Example 2.2.3. *Let $q = s^2$ and let ℓ_1, ℓ_2, ℓ_3 be three concurrent lines in $PG(2,q)$. Choose Baer sublines $\overline{\ell}_1 \subset \ell_1$, $\overline{\ell}_2 \subset \ell_2$, and $\overline{\ell}_3 \subset \ell_3$ in such a way that, for any triple of distinct $i,j,k \in \{1,2,3\}$, the Baer subplane $\mathcal{B}_{j,k} = \langle \overline{\ell_j}, \overline{\ell_k} \rangle$ meets the line ℓ_i only in the common point C. Then $\mathcal{S} = (\ell_1 \setminus \overline{\ell}_1) \cup (\ell_2 \setminus \overline{\ell}_2) \cup (\ell_3 \setminus \overline{\ell}_3)$ is a semioval which has $3(q - \sqrt{q})$ points.*

For distinct $i,j,k \in \{1,2,3\}$, the line ℓ_i is tangent to the Baer subplane $\mathcal{B}_{j,k}$. Hence $s+1$ lines of $\mathcal{B}_{j,k}$ pass through C, and exactly one line of $\mathcal{B}_{j,k}$ passes through each other point of ℓ_i. So for each point $Q \in \mathcal{L}_i$ there is a unique line of $\mathcal{B}_{j,k}$ which passes through Q. This line is t_Q, because any other element of $\mathcal{P}_Q$ does not belong to the set of lines of $\mathcal{B}_{j,k}$, and hence it meets $(\ell_j \setminus \overline{\ell_j}) \cup (\ell_k \setminus \overline{\ell_k}) = \mathcal{L}_j \cup \mathcal{L}_k$ in at least one point.

We can construct such a semioval in the following way. Let ξ be a root of an irreducible quadratic polynomial of $GF(s)[X]$. Consider $GF(q)$ as the extension of $GF(s)$ by ξ. The equations of the lines are as follows: $\ell_1 : X_2 = 0$, $\ell_2 : X_1 = 0$ and $\ell_3 : X_2 = \xi X_1$, and the Baer sublines are

$$\begin{aligned}
\overline{\ell}_1 &= \{(a,0,1) : a \in GF(s)\} \cup \{(1,0,0)\}, \\
\overline{\ell}_2 &= \{(0,b,1) : b \in GF(s)\} \cup \{(0,1,0)\}, \\
\overline{\ell}_3 &= \{(1,\xi,c\xi + c) : c \in GF(s)\} \cup \{(0,0,1)\}.
\end{aligned}$$

Let us remark that not all strong semiovals of $\mathrm{PG}(2,q)$ can be constructed this way. For instance, this follows from our description of all strong semiovals of $\mathrm{PG}(2,p^2)$ (see Theorem 2.4.5).

2.3 An algebraic description

From now on we restrict ourselves to considering semiovals in the plane $\mathrm{PG}(2,q)$, where $q > 3$ odd. Such a semioval $\mathcal{S}$ allows an algebraic description in terms of an ordered triple (R,S,T), where R, S, and T are certain subsets of $\mathrm{GF}(q)$. Namely, let us choose a system of reference for $\mathrm{PG}(2,q)$ in such a way that the lines ℓ_1, ℓ_2, and ℓ_3 have equations $X_1 = -X_3$, $X_1 = 0$, and $X_1 = X_3$, respectively. Then $C = (0,1,0) \notin \mathcal{S}$ because $q > 3$. Let

$$R = \{r \in GF(q) : (-1,r,1) \in \mathcal{L}_1\},$$

$$S = \{s \in GF(q) : (0, s, -2) \in \mathcal{L}_2\},$$
$$T = \{t \in GF(q) : (1, t, 1) \in \mathcal{L}_3\}.$$

If we denote the size of $\mathcal{L}_i$ by a, then $|R| = |S| = |T| = a$. Consider the sets R, S and T as subsets of the additive group of $GF(q)$, call it E for short. For a subset $A \subseteq E$ we put $-A = \{-u : u \in A\}$ and $A^c = E \setminus A$. Now $r + s + t = 0$ if and only if the points $(-1, r, 1), (0, s, -2)$ and $(1, t, 1)$ are collinear. Thus, $\mathcal{S}$ is a semioval if and only if

$$\begin{aligned} |S^c + u \cap -T^c| &= 1, \quad \text{if } u \in R, \\ |T^c + u \cap -R^c| &= 1, \quad \text{if } u \in S, \\ |R^c + u \cap -S^c| &= 1, \quad \text{if } u \in T. \end{aligned}$$

But for every $u \in E$,

$$|S + u \cap -T| + |S + u \cap (-T)^c| = |S + u| = a,$$

$$|S + u \cap -T^c| + |S^c + u \cap -T^c| = |-T^c| = q - a.$$

Further, if $u \in R$ then $|S + u \cap (-T)^c| = |S + u \cap -T^c|$, and so $|S^c + u \cap -T^c| = 1$ amounts to $|S + u \cap -T| = 2a - q + 1$. Similarly, if $u \in S$ then $|T^c + u \cap -R^c| = 1$ amounts to $|T + u \cap -R| = 2a - q + 1$ and if $u \in T$ then $|R^c + u \cap -S^c| = 1$ amounts to $|R + u \cap -S| = 2a - q + 1$. Therefore the above system of equations is equivalent to the following one:

$$\begin{aligned} |S + u \cap -T| &= 2a - q + 1, \quad \text{if } u \in R, \\ |T + u \cap -R| &= 2a - q + 1, \quad \text{if } u \in S, \\ |R + u \cap -S| &= 2a - q + 1, \quad \text{if } u \in T. \end{aligned} \tag{2.2}$$

2.4 Strong semiovals

Let $\mathcal{S}$ be a strong semioval in $PG(2, q)$ and let S, R, T be subsets of E which are induced by $\mathcal{S}$ in the way described in the previous section. Let $a = |R| = |S| = |T|$. Since $\mathcal{S}$ is a strong semioval, there exists a natural number k such that the number of two-secants of $\mathcal{S}$ passing through each point in $\ell_i \setminus (\mathcal{L}_i \cup \{C\})$ is equal to k. (Example 2.2.3 gives a strong semioval with $k = (\sqrt{q}-1)^2$.) So instead of (2.2) we have the following refined system

of equations

$$\begin{aligned} |S+u\cap -T| &= \begin{cases} 2a-q+1, & \text{if } u\in R,\\ k, & \text{if } u\notin R,\end{cases}\\ |T+u\cap -R| &= \begin{cases} 2a-q+1, & \text{if } u\in S,\\ k, & \text{if } u\notin S,\end{cases}\\ |R+u\cap -S| &= \begin{cases} 2a-q+1, & \text{if } u\in T,\\ k, & \text{if } u\notin T\end{cases}\end{aligned} \tag{2.3}$$

We call k the *parameter* of $\mathcal{S}$. This parameter depends on q and a, as seen below.

Proposition 2.4.1. *Let $\mathcal{S}$ be a strong semioval in $PG(2,q)$ with parameter k. If $\mathcal{S}$ consists of $3a$ points, then*

$$k = a - \frac{a}{q-a}.$$

Proof. Consider the first condition of (2.3). For a given $u \in E$, the number of pairs $(s,t) \in S \times T$ such that $s+t=-u$ is equal to $2a-q+1$ if $u \in R$, and is equal to k otherwise. Therefore, the total number of such pairs (s,t) is $(2a-q+1)|R| + k|R^c|$. From this we have $(2a-q+1)a + k(q-a) = a^2$, and so $k = a - \frac{a}{q-a}$. ■

Proposition 2.4.1 shows that $(q-a)$ divides a, and hence $(q-a)$ divides q. Thus, if $q = p^m$ then $a = p^m - p^l$, and from Theorem 2.2.2 we have $|\mathcal{S}| = 3(p^m - p^l)$ where $m/2 \le l < m$. In particular, we get the following corollary.

Corollary 2.4.2. *There is no strong semioval in $PG(2,p)$ if p is an odd prime.*

A triple of subsets R, S, T of E for which $|S| = |R| = |T| = a$ satisfying (2.3) is called a *semioval-triple* of E. Semioval-triples with maximal cardinality are closely related to factorizations of E. Let G be an additive group. The nonempty subsets $A_1, ..., A_n$ of G induce a factorization of G, if every $g \in G$ can be uniquely written in the form $g = a_1 + a_2 + \cdots + a_n$, $a_i \in A_i$. This will be expressed as $G = A_1 + A_2 + \cdots + A_n$. For more on factorizations of abelian groups, we refer the reader to [44]. We have the following necessary and sufficient condition.

Proposition 2.4.3. *Let $q = p^{2l}$, p an odd prime. If the subsets S, R and T of E having cardinality $p^{2l} - p^l$ form a semioval-triple of E, then E has factorizations $E = S^c + T^c = R^c + T^c = R^c + S^c$.*

On the other hand, if $E = A_1 + A_2 = A_2 + A_3 = A_1 + A_3$ are factorizations such that $|A_1| = |A_2| = |A_3|$, then the sets A_1^c, A_2^c and A_3^c form a semioval-triple of E.

Proof. Assume first that R, S and T of E have cardinality $p^{2l}-p^l$ and that they form a semioval-triple of E. Then $k=(p^l-1)^2$, by Proposition 2.4.1. Also $2a-q+1=(p^l-1)^2=k$, and hence (2.3) reduces to

$$|S+u\cap -T|=|T+u\cap -R|=|R+u\cap -S|=(p^l-1)^2, \text{ if } u\in E.$$

Then

$$(p^l-1)^2=|T+u\cap -S|=|T+u|-|T+u\cap -S^c|=p^{2l}-p^l-|T+u\cap -S^c|,$$

from which we get $|T\cap -S^c-u|=|T+u\cap -S^c|=p^l-1$. Thus

$$|T^c+u\cap -S^c|=|T^c\cap -S^c-u|=|-S^c-u|-|T\cap -S^c-u|=p^l-(p^l-1)=1.$$

In other words, for every $u\in E$, we have $s+t=-u$ for unique $s\in S^c$ and $t\in T^c$, so that $E=S^c+T^c$. The factorizations $E=R^c+T^c=R^c+S^c$ follow in the same way.

Conversely, let $E=A_1+A_2=A_2+A_3=A_1+A_3$ be such that $|A_1|=|A_2|=|A_3|$. Clearly, $|A_1|=|A_2|=|A_3|=p^l$. Now one only has to reverse the previous argument to deduce that the sets A_1^c, A_2^c and A_3^c form a semioval-triple. ■

The following classical result on factorizations is due to Rédei [42].

Theorem 2.4.4. [44, Theorem 1.4.1] *Let $G=A_1+\cdots+A_n$ be a factorization of the finite abelian group G such that for the identity element 0 of G, $0\in A_i$ and $|A_i|$ is a prime for each i, $1\le i\le n$. Then at least one of the factors $A_1,...,A_n$ is a subgroup of G.*

Combining together Theorem 2.4.4 and Proposition 2.4.3 we obtain a complete characterization of strong semiovals in $\mathrm{PG}(2,p^2)$, p an odd prime.

Theorem 2.4.5. *If $\mathcal{S}$ is a strong semioval in $PG(2,p^2)$, p an odd prime, and $\mathcal{S}$ is contained in the union of lines ℓ_1,ℓ_2 and ℓ_3, then $\mathcal{L}\setminus\mathcal{S}$ can be described as the point set*

$$\big\{\,(-1,a,1),(0,b,1),(1,i,ci+f(c))\colon\ a,b,c\in GF(p)\,\big\}\cup\big\{\,C\big\},\qquad(2.4)$$

where $C=(0,1,0)$, $i^2=\varepsilon$ for a non-square element ε of $GF(p)$, $GF(p^2)$ is the extension of $GF(p)$ by i, and eventually, f is a permutation of $GF(p)$.

Proof. Let $\mathcal{S}$ be a strong semioval in $\mathrm{PG}(2,p^2)$. As in Section 3 let us choose the system of reference in such a way that the lines ℓ_1, ℓ_2 and ℓ_3 have equations $X_1=-X_3$, $X_1=0$ and $X_1=X_3$, respectively, and let S, R and T be the corresponding subsets of E induced then by $\mathcal{S}$. Coordinatize the plane in such a way that the identity element 0 of E belongs to $0\in$

$R^c \cap S^c \cap T^c$. By Proposition 2.4.3 the statement that $\mathcal{S}$ is a strong semioval is equivalent to saying that E has the following factorizations:

$$E = R^c + S^c = R^c + T^c = S^c + T^c, \quad |R^c| = |S^c| = |T^c| = p.$$

By Theorem 2.4.4 it follows that at least two of the sets R^c, S^c and T^c coincide with a subgroup of E of index p. We may assume that these are R^c and S^c. Moreover, S^c and R^c may be identified with $\mathrm{GF}(p)$ and $\mathrm{GF}(p)i$, respectively. Clearly, $E = R^c + S^c$. We are going to show that $E = T^c + R^c = T^c + S^c$ if and only if

$$T = \{g(c)i + c \colon c \in GF(p)\} \tag{2.5}$$

for some permutation g of $GF(p)$. It is easy to check that if T is of the form given above, then $E = T^c + R^c = T^c + S^c$.

Conversely, assume that $E = T^c + R^c = T^c + S^c$. Let $a_1 i + b_1$ and $a_2 i + b_2$ be two elements of T, with $a_i, b_i \in GF(p)$. If $a_1 = a_2$ and $b_1 \neq b_2$, then $a_1 i = (a_1 i + b_1) + (-b_1) = (a_2 i + b_2) + (-b_2)$, which contradicts $T^c + S^c = E$. Thus $\{a \in GF(p) \colon ai + b \in T\} = GF(p)$. We also have $\{b \in GF(p) \colon ai + b \in T\} = GF(p)$, which follows from the assumption $T^c + R^c = E$ by a similar argument. These imply (2.5).

Also, we obtained that $(\ell_1 \cup \ell_2 \cup \ell_3) \setminus \mathcal{S}$ can be described as the point set

$$\big\{\, (0, b, 1), (-1, ai, 1), (1, c + g(c)i, 1) \colon\ a, b, c \in GF(p) \,\big\} \cup \big\{E_2\big\}.$$

Let ψ be the collineation of $\mathrm{PG}(2, p^2)$ defined as $\psi \colon (X_1, X_2, X_3) \mapsto (X_1, X_2, X_3)M$, where

$$M = \begin{pmatrix} 1 & \frac{i}{2} & 0 \\ 0 & 0 & i \\ 0 & \frac{i}{2} & 0 \end{pmatrix}.$$

Then the above set is mapped by ψ to the set

$$\big\{\, (0, \frac{i}{2}, bi), (-1, 0, \varepsilon a), (1, i, ci + \varepsilon g(c)) \colon\ a, b, c \in GF(p) \,\big\} \cup \big\{(0, 0, i)\big\}.$$

Note that this point set coincides with the one given in (2.4), after the substitution $f = \varepsilon g$. ■

Recall that, by Theorem 2.2.2, the size of a semioval $\mathcal{S}$ in Π_q, $q > 3$, contained in the union of three concurrent lines, is bounded above by $3\lceil q - \sqrt{q} \rceil$. In the rest of the section we consider strong semiovals $\mathcal{S}$ satisfying $|\mathcal{S}| < 3(q - \sqrt{q})$. For the existence of such a semioval we have the following divisibilty condition.

Theorem 2.4.6. *If $\mathcal{S}$ is a strong semioval of cardinality $|\mathcal{S}| = 3(p^m - p^l)$, $m/2 < l < m$, in $PG(2,q)$, $q = p^m$ odd, then*

$$(p-1)(p^{2l-m}-1)^2 \mid (p^{m-l}-1). \tag{2.6}$$

Proof. We are going to reformulate (2.3) in the language of the group algebra $\mathbb{Q}E$. Recall that $\mathbb{Q}E$ consists of formal sums $\sum_{u\in E} a_u u$, where $u \in E$ and $a_u \in \mathbb{Q}$, with addition

$$\sum_{u\in E} a_u u + \sum_{u\in E} b_u u = \sum_{u\in E} (a_u + b_u)u,$$

and multiplication

$$\sum_{u\in E} a_u u \cdot \sum_{u\in E} b_u u = \sum_{u\in E}\sum_{v\in E} (a_v b_{u-v})u.$$

For $\alpha = \sum_{u\in E} a_u u \in \mathbb{Q}E$, the multiplication of α by a scalar $a \in \mathbb{Q}$ is defined as $a\alpha = \sum_{u\in E}(aa_u)u$. We let $\alpha^\top = \sum_{u\in E} a_u(-u)$, where $-u$ is the inverse of u in E. For a subset $A \subseteq E$, the symbol A will also denote the group algebra element $\sum_{u\in A} u$.

Let R, S, and T be the sets of the semioval-triple induced by $\mathcal{S}$. Observe that (2.3) can then be reformulated in the language of $\mathbb{Q}E$ as follows (where $R^\top = \{\alpha^\top : \alpha \in R\}$, $S^\top = \{\alpha^\top : \alpha \in S\}$ and $T^\top = \{\alpha^\top : \alpha \in T\}$ form the counterparts of $-R$, $-S$ and $-T$ in $\mathbb{Q}E$, respectively):

$$\begin{aligned} S \cdot T &= (p^{m-l} - p^l)R^\top + (p^m - p^l - p^{m-l} + 1)E, \\ T \cdot R &= (p^{m-l} - p^l)S^\top + (p^m - p^l - p^{m-l} + 1)E, \\ R \cdot S &= (p^{m-l} - p^l)T^\top + (p^m - p^l - p^{m-l} + 1)E. \end{aligned} \tag{2.7}$$

For an irreducible character χ of E, the symbol χ will also denote its natural extension to $\mathbb{Q}E$ defined as $\chi(\alpha) = \sum_{u\in E} a_u \chi(u)$, for $\alpha = \sum_{u\in E} a_u u$. This is an algebra homomorphism of $\mathbb{Q}E$ into $\mathbb{Q}(\xi)$, where ξ is a complex primitive p-th root of unity. Apply now a non-principal character χ of E to (2.7). (The definition of a non-principal character, and all facts from character theory which are used here can be found, e. g., in [1].) This yields

$$\begin{aligned} \chi(S)\,\chi(T) &= (p^{m-l} - p^l)\,\chi(R^\top), \\ \chi(T)\,\chi(R) &= (p^{m-l} - p^l)\,\chi(S^\top), \\ \chi(R)\,\chi(S) &= (p^{m-l} - p^l)\,\chi(T^\top). \end{aligned} \tag{2.8}$$

Since $m/2 < l$ we have $p^{m-l} - p^l \neq 0$. Thus, from (2.8) it follows that $\chi(R) \neq 0$ implies $\chi(R \cdot R^\top) = (p^{m-l} - p^l)^2$. Therefore, $\chi(R \cdot R^\top) = 0$ or

$\chi(R \cdot R^\top) = (p^{m-l} - p^l)^2$ for every non-principle character χ of E. Assume that $\chi(R \cdot R^\top) = (p^{m-l} - p^l)^2$ for exactly s non-principal characters. Now $\chi(R \cdot R^\top) = (p^{m-l} - p^l)^2$ implies $\chi^i(R \cdot R^\top) = (p^{m-l} - p^l)^2$ for all $i \in \{1, 2, \ldots, p-1\}$. Thus, $p-1$ divides s. Set $s = s'(p-1)$.

Let $R \cdot R^\top = \sum_{u \in E} r_u u$ in $\mathbb{Q}E$. Note that $r_0 = p^m - p^l$, where 0 is the identity element of E. Denote by E^* the set of all irreducible characters of E. Then

$$\sum_{\chi \in E^*} \chi(R \cdot R^\top) = (p^m - p^l)^2 + s(p^{m-l} - p^l)^2.$$

Since $\sum_{\chi \in E^*} \chi(u) = p^m$, if $u = 0$ (the identity of E), and it is equal to 0 otherwise, we also have

$$\sum_{\chi \in E^*} \chi(R \cdot R^\top) = \sum_{\chi \in E^*} \sum_{u \in E} r_u \chi(u) = \sum_{u \in E} r_u \sum_{\chi \in E^*} \chi(u) = p^m(p^m - p^l).$$

From these we obtain

$$s' = \frac{p^{4l-2m}(p^{m-l} - 1)}{(p-1)(p^{2l-m} - 1)^2},$$

and(2.6) follows. ■

For a given p, the numbers m, l satisfying (2.6) can be described explicitly.

Lemma 2.4.7. *Let p be an odd prime, and let m and l be natural numbers such that $\frac{1}{2}m < l < m$. Then*

$$N_{p,m,l} = \frac{p^{m-l} - 1}{(p-1)(p^{2l-m} - 1)^2}$$

is a natural number if an only if

$$m = (2t_{p,\lambda,\tau} + 1)\tau \quad \text{and} \quad l = (t_{p,\lambda,\tau} + 1)\tau,$$

where λ and τ are natural numbers and

$$t_{p,\lambda,\tau} = \begin{cases} \frac{1}{2}\lambda(p-1)(p^\tau - 1), & \tau \text{ odd and } p \equiv -1 \pmod 4 \\ \lambda(p-1)(p^\tau - 1), & \text{otherwise.} \end{cases}$$

Proof. If $N_{p,m,l}$ is a natural number, then $p^{m-l} - 1$ must be divisible by $p^{2l-m} - 1$, and by a well known result from number theory, $m - l$ must be divisible by $2l - m$; that is, $m - l = t(2l - m)$ for some natural number t. For convenience, set $\tau = 2l - m$. Then

$$m = (2t + 1)\tau \quad \text{and} \quad l = (t + 1)\tau,$$

and $N_{p,m,l}$ takes the form

$$N_{p,\tau,t} = \frac{p^{t\tau}-1}{(p-1)(p^\tau-1)^2}.$$

The original question – when is $N_{p,m,l}$ a natural number – has now reduced to an equivalent one: if p is an odd prime and τ and t natural numbers, when is $N_{p,\tau,t}$ a natural number. Now $N_{p,\tau,t}$ can be written in the form

$$N_{p,\tau,t} = \frac{1}{p-1}\left[\frac{p^{(t-1)\tau}-1}{p^\tau-1} + \ldots + \frac{p^\tau-1}{p^\tau-1} + \frac{t}{p^\tau-1}\right].$$

If $N_{p,\tau,t}$ is a natural number, then the number in brackets must be a natural number. So $t = z(p^\tau-1)$ for some natural number z. Observe that $N_{p,\tau,t}$ now takes the form

$$\begin{aligned} N_{p,\tau,z} &= \frac{1}{p-1}\left[p^{(t-2)\tau} + 2p^{(t-3)\tau} + \ldots + (t-2)p^\tau + (t-1) + z\right] \\ &= \left[\frac{p^{(t-2)\tau}-1}{p-1} + 2\frac{p^{(t-3)\tau}-1}{p-1} + \ldots + (t-2)\frac{p^\tau-1}{p-1}\right] + \\ &\quad + \left[\frac{t(t-1)}{2(p-1)} + \frac{z}{p-1}\right]. \end{aligned}$$

The original problem has thus reduced to the question – for which natural numbers t and z is $N := \frac{t(t-1)}{2(p-1)} + \frac{z}{p-1}$ a natural number. We split the analysis into two cases.

First, let τ be even. Writing N in the form

$$N = z\frac{p^{\tau-1}+\ldots p+1}{2}(t-1) + \frac{z}{p-1},$$

we see that N is a natural number if and only if $z = \lambda(p-1)$ for some natural number λ. This gives m and l in terms of p, τ and λ as stated.

Suppose now that τ is odd. Writing N in the form

$$N = \left[z\frac{p^{\tau-1}+\ldots p}{2}(t-1) + z^2\frac{p^\tau-1}{2} - z\right] + \left[\frac{z}{2} + \frac{z}{p-1}\right]$$

we see that N is a natural number if and only if $u = \frac{z}{2} + \frac{z}{p-1}$ is a natural number. Thus,

$$z = 2u - \frac{4u}{p+1},$$

which brings us to considering the congruence class of the odd prime p modulo 4. If $p = 4s+1$, then $z = 2u - \frac{2u}{2s+1}$. So $u = \lambda(2s+1)$ and

consequently, $z = \lambda(p-1)$. This gives m and l as stated in the lemma. Finally, let $p = 4s-1$. Then $z = 2u - \frac{u}{s}$. Hence $u = \lambda s$ and consequently, $z = \frac{1}{2}\lambda(p-1)$. Again, this gives m and l as stated, and the proof is complete. ■

Observe that, with the notation of Lemma 2.4.7, we have $t_{p,\lambda,\tau} \geq \frac{1}{2}(p-1)^2$ for $p \equiv -1 \pmod 4$, and $t_{p,\lambda,\tau} \geq (p-1)^2$ for $p \equiv 1 \pmod 4$. Thus, if $N_{p,\tau,t}$ is a natural number then $m \geq (p-1)^2 + 1$ for $p \equiv -1 \pmod 4$, and $m \geq 2(p-1)^2 + 1$ for $p \equiv 1 \pmod 4$. We conclude the paper with the following corollary of the divisibilty condition of Theorem 2.4.6.

Corollary 2.4.8. *If $\mathcal{S}$ is a strong semioval in $PG(2, p^m)$, where p is an odd prime, and*

$$m \leq \begin{cases} (p-1)^2 & p \equiv -1 \pmod 4 \\ 2(p-1)^2 & p \equiv 1 \pmod 4, \end{cases}$$

then $|\mathcal{S}| = 3(q - \sqrt{q})$.

Recently B. Csajbók and Gy. Kiss in [15] using a bit more complicated arguments from additive group theory could generalize our non-existance results. They proved the following:

Theorem 2.4.9. *Let $\mathcal{S}$ be a strong semioval in $PG(2, p^r)$, p an odd prime. Then the followings hold.*

1. *If $r = 2l$, then $\mathcal{S}$ contains $3(p^{2l} - p^l)$ points.*
2. *If $r = 2l+1$ and $p > 7$, then there is no strong semioval in $PG(2, p^r)$.*
3. *If $r = 2l+1$ and $p = 3, 5$ or 7, then $\mathcal{S}$ contains $3(p^{2l+1} - p^{l+1})$ points.*

Combining the results of 2.4.9 and 2.4.6 one can easily see the following

Theorem 2.4.10. *Let $\mathcal{S}$ be a strong semioval in $PG(2, p^r)$ where p is an odd prime and r is odd. Then $p = 3$, and $r = 4t+1$ or $p = 5$, and $r = 32t+1$ or $p = 7$, and $r = 36t+1$, where t is a positive integer.*

Proof. Assuming that p is an odd prime and r is odd the only three possibilities are $p = 3, 5$ or 7, and the divisibility condition in 2.4.6 gives the following:

$$(p-1)^3 \mid p^{\frac{r-1}{2}} - 1.$$

Substituting $a = p-1$ and $k = \frac{r-1}{2}$ the condition to be checked turns into the condition $a^3 \mid (a+1)^k - 1$. Using the binomial theorem it gives the necessary divisibility conditions for r. ■

These results, our example for strong semiovals 2.2.3 altogether and the fact that in the third case of Theorem 2.4.9 there is no known example supports our concluding conjecture.

Conjecture 2.4.11. *The projective plane $PG(2, q)$, q odd, contains strong semiovals if and only if q is a square.*

Chapter 3

Large Cayley graphs of given degree and diameter

3.1 Introduction

A simple finite graph Γ is a (Δ, D)-*graph* if it has maximum degree Δ, and diameter at most D. The (Δ, D)-*problem* (or *degree/diameter problem*) is to determine the largest possible number of vertices that Γ can have. Denote this number by $n(\Delta, D)$. There is a straightforward on $n(\Delta, D)$. Trivially, if $\Delta = 1$ then $D = 1$ and $n(1, 1) = 2$; in what follows we therefore assume that $\Delta \geq 2$.
Let v be a vertex of the graph Γ and let n_i, be the number of vertices at distance i from v. Since a vertex at distance $i \geq 1$i from v can be adjacent to at most $\Delta - 1$ vertices at distance $i+1$ from v, we have $n_{i+1} \leq (\Delta - 1)n_i$, for all $1 \leq i \leq D - 1$. Since $n_1 \leq \Delta$, it follows that $n_i \leq \Delta(\Delta - 1)^{i-1}$, for all $1 \leq i \leq D$.
Therefore if $\Delta > 2$, then

$$n(\Delta, D) = \sum_{i=0}^{D} n_i \leq \frac{\Delta(\Delta - 1)^D - 2}{\Delta - 2} \tag{3.1}$$

The bound was named after E. F. Moore who first proposed the problem, as mentioned in [27] . A graph whose order is equal to the Moore bound is called a Moore graph; such a graph is necessarily regular of degree Δ.
The study of Moore graphs was initiated by Hoffman and Singleton. Their pioneering paper [27] was devoted to Moore graphs of diameter 2 and 3. In the case of diameter $D = 2$, they proved that Moore graphs exist for $\Delta = 2, 3, 7$ and possibly 57 but for no other degrees, and that for the first three values of Δ the graphs are unique. For $D = 3$ they showed that the unique Moore graph is the heptagon (for $\Delta = 2$).

It turns out that no Moore graphs exist for the parameters $\Delta \geq 3$ and $D \geq 3$. This was proved by Bannai and Ito in [3].

The study of large graphs of given degree and diameter has often been restricted to special classes of graphs. If in addition Γ is required to be vertex-transitive, then the only known general lower bound is given as

$$n(\Delta, 2) \geq \left\lfloor \frac{\Delta + 2}{2} \right\rfloor \cdot \left\lceil \frac{\Delta + 2}{2} \right\rceil. \tag{3.2}$$

This is obtained by choosing Γ to be the Cayley graph $\mathrm{Cay}(\mathbb{Z}_a \times \mathbb{Z}_b, S)$, where $a = \lfloor \frac{\Delta+2}{2} \rfloor$, $b = \lceil \frac{\Delta+2}{2} \rceil$, and $S = \{ (x,0), (0,y) \mid x \in \mathbb{Z}_a \setminus \{0\}, y \in \mathbb{Z}_b \setminus \{0\} \}$.
Here we recall the concept of a Cayley graph:

Definition 3.1.1. *Let G be an additive group and $S \subseteq G$ such that $0 \notin S$, and $S = -S := \{-x \mid x \in S\}$, the Cayley graph $\Gamma(G, S)$ is the graph having vertex-set G, and edges $\{x, x+s\}$, $x \in G$, $s \in S$. The set S is called the connection set of the graph.*

If $\Delta = kD+m$, where k, m are integers and $0 \leq m < D$, then a straightforward generalization of this construction results in a Cayley (Δ, D)-graph of order

$$\left\lfloor \frac{\Delta + D}{D} \right\rfloor^{D-m} \cdot \left\lceil \frac{\Delta + D}{D} \right\rceil^{m}. \tag{3.3}$$

Throughout this chapter we will refer these graphs as GCCG-graphs (General Construction from Cyclic Groups). For special values of the parameters, (3.2) and (3.3) have been improved using various constructions. For more on the topic, we refer to [49, 39].

In this chapter we restrict our attention to the class of linear Cayley graphs. We present some constructions where the resulting graphs improve the lower bounds (3.2) and (3.3). For small number of vertices these are also compared to the known largest vertex transitive graphs having the same degree and diameter.

Let V denote the n-dimensional vector space over the finite field $\mathbb{F}_q$ of q elements, where $q = p^e$ for a prime p. For $S \subseteq V$ such that $0 \notin S$, and $S = -S := \{-x \mid x \in S\}$, the Cayley graph $\mathrm{Cay}(V, S)$ is the graph having vertex-set V, and edges $\{x, x+s\}$, $x \in V$, $s \in S$. A Cayley graph $\mathrm{Cay}(V, S)$ is said to be *linear*, [23, pp. 243] if $S = \alpha S := \{\alpha x \mid x \in S\}$ for all nonzero scalars $\alpha \in \mathbb{F}_q$. In this case $S \cup \{0\}$ is a union of 1-dimensional subspaces, and therefore, it can also be regarded as a point set in the projective space $\mathrm{PG}(n-1, q)$. Conversely, any point set $\mathcal{P}$ in $\mathrm{PG}(n-1, q)$ gives rise to a linear Cayley graph, namely the one having connection set $\{x \in V \setminus \{0\} \mid \langle x \rangle \in \mathcal{P}\}$. We denote this graph by $\Gamma(\mathcal{P})$. Given an arbitrary point set $\mathcal{P}$ in $\mathrm{PG}(n, q)$,

$\langle \mathcal{P} \rangle$ denotes the projective subspace generated by the points in $\mathcal{P}$, and $\binom{\mathcal{P}}{k}$ ($k \in \mathbb{N}$) is the set of all subsets of $\mathcal{P}$ having cardinality k. The degree and diameter of linear Cayley graphs are given in the next proposition.

Proposition 3.1.2. *Let $\mathcal{P}$ be a set of k points in $\mathrm{PG}(n,q)$ with $\langle \mathcal{P} \rangle = \mathrm{PG}(n,q)$. Then $\Gamma(\mathcal{P})$ has q^{n+1} vertices, with degree $k(q-1)$, and with diameter*

$$D = \min \left\{ \, d \mid \cup_{\mathcal{X} \in \binom{\mathcal{P}}{d}} \langle \mathcal{X} \rangle = \mathrm{PG}(n,q) \, \right\}. \tag{3.4}$$

Proof. Let $\Gamma = \Gamma(\mathcal{P})$. It is immediate from its definition that Γ has q^{n+1} vertices and that its degree is equal to $k(q-1)$. Now let V denote the $(n+1)$-dimensional vector space over $\mathbb{F}_q$. Being a Cayley graph, Γ is automatically vertex-transitive, and so its diameter is the maximal distance $\delta_\Gamma(0,x)$ where $0 \in V$, and x runs over V. By δ_Γ we denote the usual distance function of Γ.

Let $x \in V \setminus \{0\}$, and let $P = \langle x \rangle$ be the corresponding point in $\mathrm{PG}(n,q)$. It can be seen that $\delta_\Gamma(0,x) = k$ where k is the minimal number of independent points $P_1, \ldots, P_k \in \mathcal{P}$ such that $P \in \langle P_1, \ldots, P_k \rangle$. Now, (3.4) shows that $\delta_\Gamma(0,x) \leq D$ for every $x \in V$, in particular, the diameter of Γ is at most D.

On the other hand, by (3.4), there exists a $Q \in \mathrm{PG}(n,q)$ for which $Q \notin \langle P_1, \ldots, P_{D-1} \rangle$ for any $P_1, \ldots, P_{D-1} \in \mathcal{P}$. Thus if y is an element of V with $\langle y \rangle = Q$, then $\delta_\Gamma(0,y) \geq D$. Therefore, the diameter of Γ cannot be less than D, which completes the proof.

■

Once the number of vertices and the diameter for $\Gamma(\mathcal{P})$ are fixed to be q^{n+1} and D, respectively, our task becomes to search for the smallest possible point set $\mathcal{P}$ for which

$$\cup_{\mathcal{X} \in \binom{\mathcal{P}}{D}} \langle \mathcal{X} \rangle = \mathrm{PG}(n,q).$$

A point set having this property is called a *(D-1)-saturating set*. In order to have proper graphs for our purposes in our following constructions we will use saturating sets of projective spaces.

3.2 The constructions

If $D = 2$, then a 1-saturating set $\mathcal{P}$ is a set of points of $\mathrm{PG}(n,q)$ such that the union of lines joining pairs of points of $\mathcal{P}$ covers the whole space. Assume that $n = 2$. If $\mathcal{P}$ contains k points, then the graph has degree $k(q-1)$ and the number of vertices is q^3. Hence this is better than the

general lower bound (3.2) if and only if $q^3 > (k(q-1)+2)^2/4$, which is equivalent to

$$2\sqrt{q} + \frac{2}{\sqrt{q}+1} > k. \tag{3.5}$$

There are two known general constructions for 1-saturating sets in the plane: complete arcs and double blocking sets of Baer subplanes.

If q is a square, and $\Pi_{\sqrt{q}}$ is a Baer subplane of $\mathrm{PG}(2,q)$, of order $\sqrt{q}$, then each point of $\mathrm{PG}(2,q) \setminus \Pi_{\sqrt{q}}$ is incident with exactly one line of $\Pi_{\sqrt{q}}$. A double blocking set of a plane meets each line of the plane in at least two points. Hence a double blocking set of $\Pi_{\sqrt{q}}$ is a 1-saturating set of $\mathrm{PG}(2,q)$. The cardinality of a double blocking set of $\Pi_{\sqrt{q}}$ is at least $2(\sqrt{q} + \sqrt[4]{q} + 1)$. This is greater than the bound given in (3.5), hence we cannot construct good graphs from these sets.
It turned out that another structure from finite geometry is more useable for us.

Definition 3.2.1. *A pointset $\mathcal{K}$ is a k-arc if it is a set of k points such that no three of them are collinear. It is a complete k-arc if moreover there is no $(k+1)$-arc containing $\mathcal{K}$.*

Thus a complete k-arc $\mathcal{K}$ is a 1-saturating set, because if a point P would not be covered by the secants of $\mathcal{K}$, then $\mathcal{K} \cup \{P\}$ would be a $(k+1)$-arc. The cardinality of the smallest complete arc in $\mathrm{PG}(2,q)$ is denoted by $t_2(2,q)$. For the known values of $t_2(2,q)$ we refer to [18]. The general lower bounds are $t_2(2,q) > \sqrt{2q} + 1$ for arbitrary q and $t_2(2,q) > \sqrt{3q} + 1/2$ for $q = p^i$, $i = 1,2,3$. But unfortunately the known complete arcs have bigger cardinality. The inequality

$$t_2(2,q) < 2\sqrt{q} + \frac{2}{\sqrt{q}+1}$$

is satisfied only for $q = 8, 9, 11$ and 13. Table 1 gives the corresponding values of $t_2(2,q)$ and the parameters of the graphs arising from these arcs.

q	$t_2(2,q)$	D	Δ	number of vertices of Γ	$\left\lfloor \frac{\Delta+2}{2} \right\rfloor \cdot \left\lceil \frac{\Delta+2}{2} \right\rceil$.
8	6	2	42	512	484
9	6	2	48	729	625
11	7	2	70	1331	1296
13	8	2	96	2197	2116

Table 1

Besides complete arcs and double blocking sets of Baer subplanes another class of small 1-saturating sets in $\mathrm{PG}(2,p)$ was examined by computer. These point sets are contained in 3 concurrent lines. For small prime orders $p = 11, 13, 17, 19$, using a simple back-track algorithm we found 1-saturating sets of this type with cardinality $10, 11, 13$ and 14, respectively. The corresponding graphs do not improve the bound in (3.2).

Now let $n > 2$. Then a set of k points such that no three of them are collinear is called k-cap. A k-cap is complete, if it is not contained in any $(k+1)$-cap. Hence complete caps in $\mathrm{PG}(n,q)$ are 1-saturating sets. For the sizes of the known complete caps we refer to [26]. There is one infinite series which gives better graphs than the GCCG-graphs. Due to Davydov and Drozhzhina-Labinskaya [17], for $n = 2m-1 > 7$ there is a complete $(27{\cdot}2^{m-4}{-}1)$-cap in $\mathrm{PG}(n,2)$. This gives a graph of degree $27{\cdot}2^{m-4}{-}1$ and of order 2^{2m}. It has much more vertices than the corresponding GCCG-graph, because

$$2^{2m} = 1024{\cdot}2^{2m-10} > 729{\cdot}2^{2m-10}{+}27{\cdot}2^{m-5} = \left\lfloor \frac{27\cdot 2^{m-4}+1}{2} \right\rfloor \cdot \left\lceil \frac{27\cdot 2^{m-4}+1}{2} \right\rceil.$$

Hence we proved the following theorem.

Theorem 3.2.2. *Let* $\Delta = 27\cdot 2^{m-4} - 1$ *and* $m > 7$. *Then*

$$n(\Delta, 2) \geq \frac{256}{729}(\Delta+1)^2.$$

■

There are sporadic examples, too. For $n = 3$ and $q = 2$ there is a complete 5-cap in $\mathrm{PG}(3,2)$. The corresponding graph has degree $\Delta = 5$ and the number of vertices is $n = 16$. The best known graph of degree 5 and diameter 2 has 24 vertices, and the best known Cayley graph has 18 vertices [2], so in this case there are bigger graphs. For $q = 3, 4$ and 5 the smallest complete caps in $\mathrm{PG}(3,q)$ have $2(q+1)$ points. The corresponding graphs have the same parameters as the GCCG-graphs.

For $n = 4$ and $q = 2, 3, 4$ there are complete caps in $\mathrm{PG}(4,q)$ with cardinalities 9, 11 and 20, respectively. For $n = 5$ and $q = 2, 3$ there are complete caps in $\mathrm{PG}(5,q)$ with cardinalities 13 and 22. The corresponding graphs have more vertices than the previously known examples. Table 2 gives the parameters of the graphs arising from these caps.

projective space	size of the complete cap	D	Δ	number of vertices of Γ	$\left\lfloor \frac{\Delta+2}{2} \right\rfloor \cdot \left\lceil \frac{\Delta+2}{2} \right\rceil$.
PG(4, 2)	9	2	9	32	30
PG(4, 3)	11	2	22	243	144
PG(4, 4)	20	2	60	1024	961
PG(5, 2)	13	2	13	64	56
PG(5, 3)	22	2	44	729	529

Table 2

In PG$(3, q)$, $q > 3$, the smallest known 1-saturating set has $2q+1$ points [16]. Let π be a plane, Ω be an oval in π, P be a point of Ω, for q even let $N \in \pi$ be the nucleus of Ω, for q odd let $N \in \pi$ be a point such that the line NP is the tangent to Ω at P, and finally let ℓ be a line such that $\ell \cap \pi = \{P\}$. Then it is easy to check that $(\Omega \cup \ell \cup \{N\}) \setminus \{P\}$ is a 1-saturating set in PG$(3, q)$. The corresponding graph has degree $\Delta = 2q^2 - q - 1$, and the number of its vertices is $q^4 > (\Delta + \sqrt{\Delta/2} + 5/4)^2/4$. Hence we proved the following theorem.

Theorem 3.2.3. *Let $q > 3$ be a prime power and let $\Delta = 2q^2 - q - 1$. Then*

$$n(\Delta, 2) > \frac{1}{4}\left(\Delta + \sqrt{\frac{\Delta}{2}} + \frac{5}{4}\right)^2.$$

■

Let ℓ_1 and ℓ_2 be two skew lines in PG$(3, q)$. If P is any point not on $\ell_1 \cup \ell_2$, then the plane generated by P and ℓ_1 meets ℓ_2 in a unique point T_2, and the line PT_2 meets ℓ_1 in a unique point T_1. Hence the line T_1T_2 contains P, so the set of points of $\ell_1 \cup \ell_2$ is a 1-saturating set in PG$(3, q)$. The corresponding graph has degree $\Delta = 2(q^2 - 1)$, and the number of its vertices is $q^4 = \big((\Delta + 2)/2\big)^2$. Hence this construction gives graphs having the same parameters as the GCCG-graphs.

A straightforward generalization of the skew line construction is the following. Let $\ell_1, \ell_2, \ldots, \ell_m$ be a set of m lines whose union spans PG$(2m-1, q)$. Then the set of points of $\cup_{i=1}^{m} \ell_i$ is an $(m-1)$-saturating set and the corresponding graph has parameters $D = m$, $\Delta = 2m(q^2 - 1)$, and the number of its vertices is q^{2m}. These parameters are the same as the parameters of the GCCG-graphs.

Another class of examples for $(D-1)$-saturating sets in PG(D, q) is the class of complete arcs. These objects are generalizations of the planar arcs. A point set $\mathcal{K}$ is a complete k-arc in PG(D, q) if no D points of $\mathcal{K}$ lie in a hyperplane, and there is no $(k+1)$-arc containing $\mathcal{K}$. The corresponding

graph has degree $k(q-1)$ and the number of vertices is q^{D+1}. Hence this is better than the known general lower bound if and only if

$$q^{D+1} > \left(\frac{k(q-1)+D}{D}\right)^D, \quad \text{that is} \quad k < \frac{D(q\sqrt[D]{q}-1)}{q-1}. \tag{3.6}$$

The typical examples for complete arcs are the normal rational curves, and almost all of the known complete arcs are normal rational curves, or subsets of these curves. There is only one known complete k-arc which satisfies (3.6). This is a normal rational curve in $\mathrm{PG}(4,3)$. The corresponding graph has degree $\Delta = 15$, diameter $D = 3$ and the number of its vertices is 256.

Chapter 4

Rose window graphs underlying rotary maps

4.1 Preliminaries

4.1.1 Maps

A *map* $\mathcal{M}$ is an embedding of a finite connected graph Γ into a surface so that it divides the surface into simply-connected regions, called the *faces* of $\mathcal{M}$. To each face f there is associated a closed walk of Γ with edges surrounding f, to which we shall also refer as a face of $\mathcal{M}$. An *automorphism* of $\mathcal{M}$ is an automorphism of Γ which preserves its faces. Following [48], $\mathcal{M}$ is called *rotary* if it admits automorphisms R and S with the property that R cyclically permutes the consecutive edges of a face f (as a one-step rotation of f), and S cyclically permutes the consecutive edges incident to some vertex v of f (as a one-step rotations of the neighbors of v). In this case the automorphism group $\mathrm{Aut}(\mathcal{M})$ of $\mathcal{M}$ acts transitively on the vertex set, edge set, and face set. We remark that the existence of R ensures that the boundary cycle of f is a so called consistent cycle of Γ, for details about this concept we refer the reader to [6, 14, 38].

If a rotary map also contains an automorphism T which 'flips' an edge e of f, and preserves f, then we say that $\mathcal{M}$ is *reflexible*. On the other hand, if no such automorphism T exists, then $\mathcal{M}$ is called *chiral*. Equivalent terminologies are orientable-regular and regular, see [21]. Namely, a rotary map is a map that is either orientable-regular or regular, whereas a reflexible map is regular map. One of the central questions regarding maps is the following: which graphs admit an embedding onto some closed surface as a rotary map (see [7, page 130]).

Throughout this chapter graphs are simple, finite and undirected. Given a graph Γ, we let $V(\Gamma)$, $E(\Gamma)$, $A(\Gamma)$ and $\mathrm{Aut}(\Gamma)$ be the vertex set, the edge set, the arc set and the automorphism group of Γ, respectively. For adjacent vertices u and v in Γ, we write $u \sim v$ and denote the corresponding edge by uv, and the arc from u to v by (u, v). If $u, v \in V(\Gamma)$ then $N_\Gamma(u)$ denotes the set of neighbors of u and $d_\Gamma(u, v)$ denotes the distance between u and v in Γ. For a subset U of $V(\Gamma)$ the subgraph of Γ induced by U will be denoted by $\Gamma[U]$. For a partition $\mathcal{W}$ of $V(\Gamma)$, we let $\Gamma/\mathcal{W}$ be the associated *quotient graph* of Γ relative to $\mathcal{W}$, that is, the graph with vertex set $\mathcal{W}$ and edge set induced naturally by the edge set $E(\Gamma)$. In the case when $\mathcal{W}$ corresponds to the set of orbits of a subgroup N of $\mathrm{Aut}(\Gamma)$, the symbol $\Gamma/\mathcal{W}$ will be replaced by Γ/N. A subgroup $G \leq \mathrm{Aut}(\Gamma)$ is said to be *vertex-transitive*, *edge-transitive* or *arc-transitive* provided it acts transitively on the set of vertices, set of edges or set of arcs of Γ, respectively. The graph Γ is said to be *vertex-transitive*, *edge-transitive*, or *arc-transitive* if its automorphism group is vertex-transitive, edge-transitive or arc-transitive, respectively.

Let Γ be a graph and $G \leq \mathrm{Aut}(\Gamma)$. A walk $\vec{D} = (u_0, \ldots, u_r)$ in X is called *G-consistent* (or just *consistent* if $G = \mathrm{Aut}(\Gamma)$) if there exists $g \in G$ such that $u_i^g = u_{i+1}$ for $i \in \{0, 1, \ldots, r-1\}$. The automorphism g is called a *shunt automorphism* for $\vec{D}$. If $\vec{D}$ is a simple closed walk then we say that $\vec{D}$ is a *G-consistent oriented cycle*. The underlying nonoriented cycle of $\vec{D}$ is called a *G-consistent cycle* and is denoted by D. The following result of Conway [14] implies that an arc-transitive group G of automorphisms of a quartic graph has exactly three orbits in its action on the set of all G-consistent oriented cycles. A written proof of this result is given by Biggs in [6] (see also [38]).

Proposition 4.1.1. [6, 14] *Let G be a group of automorphisms of a d-valent graph Γ ($d \geq 2$). Assume that G is arc-transitive. Let Ω be the set of all G-consistent oriented cycles in Γ. Then G has exactly $d-1$ orbits in its action on Ω.*

The following proposition gives a criterion of embeddings of graphs onto orientable surfaces as rotary maps in terms of their automorphism groups.

Proposition 4.1.2. [21, Theorem 1] *A connected graph Γ of valency at least 3 underlies a rotary map on an orientable surface if and only if there exists $K \leq \mathrm{Aut}(\Gamma)$ satisfying the following properties.*

1. *K is transitive on the set of arcs of Γ.*
2. *The vertex stabilizer K_v of a vertex v of Γ is cyclic.*

The graph Γ with the group K in the above proposition gives rise to a rotary map $\mathcal{M}$ in the following manner (see the proof of [21, Theorem 1]). Let v be a fixed vertex of Γ. For $u \in V(\Gamma)$ choose an automorphism $\alpha \in K$ such that $u = v^\alpha$. The conjugate subgroup $K_v^\alpha = \alpha^{-1} K_v \alpha$ cyclically permutes the arcs emanating from u, which as a cycle in $\mathrm{Sym}(A(\Gamma))$ does not depend on the choice of α. Denote this cycle by R_u, and let the permutations R and I of the arc set $A(\Gamma)$ be defined by

$$R = \prod_{u \in V(\Gamma)} R_u \quad \text{and} \quad I = \prod_{uv \in E(\Gamma)} ((u,v),(v,u)).$$

Then the face boundaries of $\mathcal{M}$ are given by the orbits of RI. It follows that $K \leq \mathrm{Aut}(\mathcal{M})$. Further, conditions (i) and (ii) imply that K is regular on the arc set $A(\Gamma)$, so we have $|K| = |A(\Gamma)|$. Now the map $\mathcal{M}$ is reflexible if and only if $|\mathrm{Aut}(\mathcal{M})| = 2|K| = 2|A(\Gamma)|$. Eventually observe that any conjugate subgroup K^β of $\mathrm{Aut}(\Gamma)$ satisfies the conditions (i) and (ii); and further that the map induced by K^β is reflexible if and only if $\mathcal{M}$ is reflexible. The analogous criterion of embeddings of graphs onto surfaces as reflexible maps is the following.

Proposition 4.1.3. [21, Theorem 3] *A connected graph Γ of valency at least 3 underlies a reflexible map if and only if there exists $K \leq \mathrm{Aut}(\Gamma)$ satisfying the following properties.*

1. *The subgroup K is transitive on the set of arcs of Γ.*
2. *The vertex stabilizer K_v of a vertex v of Γ is a dihedral group in which the cyclic subgroup of index 2 acts regularly on the arcs emanating from v.*
3. *The edge stabilizer K_e of an edge e of Γ is a dihedral group of order 4.*

4.1.2 Coverings and voltage graphs

A graph $\widetilde{\Gamma}$ is called a *covering* of a graph Γ with a *projection* $p\colon \widetilde{\Gamma} \to \Gamma$, if p is a surjection from $V(\widetilde{\Gamma})$ to $V(\Gamma)$ which is locally bijective, that is, $p|_{N(\widetilde{v})} \to N(v)$ is a bijection for any vertex $v \in V(\Gamma)$ and $\widetilde{v} \in p^{-1}(v)$. The graph $\widetilde{\Gamma}$ is also called a *covering graph* and Γ is the *base graph*. A covering $\widetilde{\Gamma}$ of Γ with projection p is said to be *regular* (or *K-covering*) if there is a semiregular subgroup K of $\mathrm{Aut}(\widetilde{\Gamma})$ such that Γ is isomorphic to the quotient $\widetilde{\Gamma}/K$, say by h, and the quotient map $\widetilde{\Gamma} \to \widetilde{\Gamma}/K$ is the composition ph of p and h. If $\widetilde{\Gamma}$ is connected, then K is also called the *covering transformation group*; moreover if K is cyclic then $\widetilde{\Gamma}$ is also called a *cyclic covering* of Γ.

A combinatorial description of a K-covering was introduced through a voltage graph by Gross and Tucker [25]. Let Γ be a graph and K be a finite group. By x^{-1} we mean the reverse arc of an arc $x \in A(\Gamma)$. A *voltage assignment* (or, a *K-voltage assignment*) of Γ is a mapping $\zeta\colon A(\Gamma) \to K$ with the property that $\zeta(x^{-1}) = \zeta(x)^{-1}$ for any $x \in A(\Gamma)$. The values of ζ are called *voltages*, and K is the *voltage group*. The *voltage graph* $\Gamma \times_\zeta K$ derived from a voltage assignment $\zeta\colon A(\Gamma) \to K$ has vertex set $V(\Gamma) \times K$, and edges of the form $(u, g)(v, \zeta(x)g)$, where $x = (u, v) \in A(\Gamma)$. Clearly, $\Gamma \times_\zeta K$ is a covering of Γ with the first coordinate projection. By letting K act on $V(\Gamma \times_\zeta K)$ as $(u, g)^{g'} = (u, gg')$, $(u, g) \in V(\Gamma \times_\zeta K)$, $g' \in K$, we obtain a semiregular group of automorphisms of $\Gamma \times_\zeta K$, showing that $\Gamma \times_\zeta K$ can in fact be viewed as a K-covering. Given a spanning tree T of Γ, the voltage assignment ζ is said to be *T-reduced* if the voltages on the tree arcs equal the identity element. In [25] it is shown that every regular covering $\tilde{\Gamma}$ of a graph Γ can be derived from a T-reduced voltage assignment ζ with respect to an arbitrary fixed spanning tree T of Γ.

Let $\tilde{\Gamma}$ be a K-covering of Γ with a projection p. If $\alpha \in \mathrm{Aut}(\Gamma)$ and $\widetilde{\alpha} \in \mathrm{Aut}(\widetilde{\Gamma})$ satisfy $\widetilde{\alpha}p = p\alpha$ then we call $\widetilde{\alpha}$ a *lift* of α, and α the *projection* of $\widetilde{\alpha}$. If the covering graph $\widetilde{X}$ is connected then the covering transformation group K is the lift of the trivial subgroup of $\mathrm{Aut}(\Gamma)$. Note that a subgroup $G \leq \mathrm{Aut}(\widetilde{\Gamma})$ projects if and only if the partition of $V(\Gamma)$ into the orbits of K is G-invariant.

The problem of determining whether an automorphism α of Γ lifts or not can be grasped in terms of voltages as follows. Observe that a voltage assignment on arcs extends to a voltage assignment on walks in a natural way. We define a function $\bar{\alpha}$ from the set of voltages of fundamental closed walks based at a fixed vertex $v \in V(\Gamma)$ to the voltage group K by $\bar{\alpha}(\zeta(C)) = \zeta(C^\alpha)$, where C ranges over all fundamental closed walk at the base vertex v, and $\zeta(C)$ and $\zeta(C^\alpha)$ are the voltages of C and C^α, respectively. Note that if K is abelian then $\bar{\alpha}$ does not depend on the choice of the base vertex, and the fundamental closed walks at v can be substituted by the fundamental cycles generated by the cotree arcs of Γ. The next proposition is a special case of [35, Theorem 4.2].

Proposition 4.1.4. [35] *Let $\Gamma \times_\zeta K$ be a connected K-covering. Then an automorphism α of Γ lifts if and only if $\bar{\alpha}$ extends to an automorphism of K.*

The following result may be deduced from [36, Corollary 3.3].

Proposition 4.1.5. [36] *Let $\tilde{\Gamma}_1 = \Gamma \times_\zeta K$ and $\tilde{\Gamma}_2 = \Gamma \times_{\zeta'} K$ be two connected K-coverings of a graph Γ where ζ and ζ' are T-reduced voltage assignments.*

Then $\tilde{\Gamma}_1$ and $\tilde{\Gamma}_2$ are isomorphic if and only if there exist an automorphism $\gamma \in \mathrm{Aut}(K)$ and an automorphism $g \in \mathrm{Aut}(\Gamma)$ such that $\gamma(\zeta(C)) = \zeta'(C^g)$ for every fundamental cycle C with respect to the spanning tree T in Γ.

4.2 Rose window graphs

Introduced by Wilson [47], the rose window graphs are defined in the following way.

Definition 4.2.1. *Given natural numbers $n \geq 3$ and $1 \leq a, r \leq n-1$, the* rose window graph *$R_n(a, r)$ has vertex set $\{x_i \mid i \in \mathbb{Z}_n\} \cup \{y_i \mid i \in \mathbb{Z}_n\}$ and edge set:*

$$\{\{x_i, x_{i+1}\} \mid i \in \mathbb{Z}_n\} \cup \{\{y_i, y_{i+r}\} \mid i \in \mathbb{Z}_n\} \cup \{\{x_i, y_i\} \mid i \in \mathbb{Z}_n\} \cup \{\{x_{i+a}, y_i\} \mid i \in \mathbb{Z}_n\}.$$

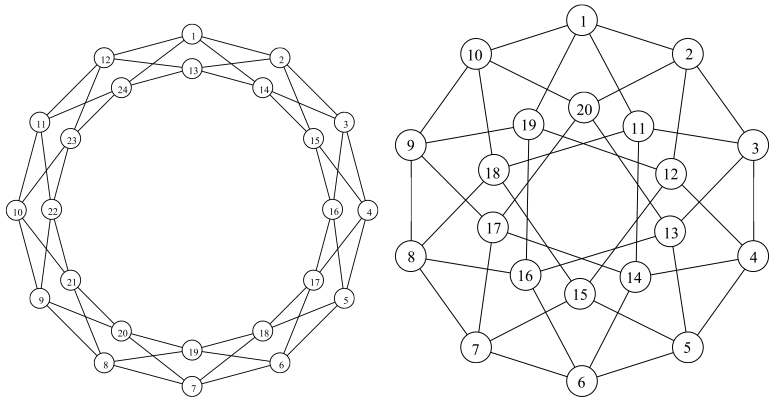

Figure 4.1: $R_{12}(2,1)$ and $R_{10}(2,3)$ rose window graphs

Wilson's initial interest in rose window graphs arose in the context of graph embeddings into surfaces. In particular, the following three open questions about rose window graphs are posed in [47].

Question 4.2.2. [47] *Given natural numbers $n \geq 3$ and $1 \leq a, r \leq n-1$,*

(i) for which n, a and r is $R_n(a, r)$ edge-transitive;
(ii) when $R_n(a, r)$ is edge-transitive, what is the order of its automorphism group;
(iii) for which n, a and r is $R_n(a, r)$ the underlying graph of a rotary map?

Wilson [47] identified the following four families **(a)**-**(d)** of edge-transitive rose window graphs $R_n(a,r)$ given below and conjectured that these graphs exhaust the whole class of edge-transitive rose window graphs. The conjecture was confirmed by Kovács, Kutnar and Marušič [33].

- **(a)** $R_n(2,1)$;
- **(b)** $R_{2m}(m-2,m-1)$;
- **(c)** $R_{12m}(3m+2,3m-1)$ and $R_{12m}(3m-2,3m+1)$;
- **(d)** $R_{2m}(2b,r)$, where $b^2=\pm 1 \pmod m$, $2\le 2b\le m$, and $r\in\{1,m-1\}$ is odd.

Observe that family **(a)** is contained in family **(d)** and that each graph $R_n(a,r)$ in families **(a)**-**(d)** satisfies the condition $1\le a,r\le n/2$. The latter is is a natural restriction by the following easy observations (see also [47]):

$$R_n(a,r)\cong R_n(n-a,r) \text{ and } R_n(a,r)=R_n(a,n-r).$$

Furthermore, there are examples of isomorphic rose window graphs in families **(a)**-**(d)** which have different parameters. For instance, the two graphs in family **(c)** are isomorphic if m is divisible by 4.

The main goal of this chapter is to confirm this conjecture by proving the following theorem.

Theorem 4.2.3. *Let $\Gamma=R_n(a,r)$ be a rose window graph underlying a rotary map $\mathcal{M}$, $1\le a,r\le n/2$. Then one of the following holds.*

1. *$\mathcal{M}$ is reflexible, and*
   - *(a)* $\Gamma=R_n(2,1)$, $\gcd(n,12)>2$,
   - *(b)* $\Gamma=R_{2m}(m-2,m-1)$, $\gcd(m,60)>3$,
   - *(c)* $\Gamma=R_{12m}(3m+2,3m-1)$ *or* $R_{12m}(3m-2,3m+1)$, $m\equiv 2 \pmod 4$.
2. *$\mathcal{M}$ is chiral, and $\Gamma=R_{2m}(2b,r)$, $m>2$, $2\le 2b\le m$, $b^2\equiv -1 \pmod m$, and $r=1$, or $r=m-1$ and m is even.*

4.3 Automorphism groups of edge-transitive graphs $R_n(a,r)$

Let Γ be the rose window graph $R_n(a,r)$. Then it can be seen that the permutations ρ and μ of $V(\Gamma)$,

$$\rho=(x_0,\,x_1,\ldots,x_{n-1})(y_0,\,y_1,\ldots,y_{n-1}) \quad\text{and}\quad \mu=\prod_{i=0}^{n-1}(x_i,\,x_{n-i})(y_i,\,y_{n-i-a}),$$

are always automorphisms of Γ. In addition, the group $\langle \rho, \mu \rangle$ is isomorphic to the dihedral group D_n of order $2n$. Observe also that the automorphism $\mu\rho$ reverses the edge x_0x_1, which implies that Γ is edge-transitive if and only if it is arc-transitive. Occasionally, when we wish to emphasize that ρ and μ are automorphisms of a particular graph Γ, we shall also write ρ_Γ and μ_Γ instead of ρ and μ.

We use the following notation. Let $E = \langle \varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{l-1} \rangle \cong \mathbb{Z}_2^l$ be the elementary abelian 2-group. Then for a divisor d of l, and for a subset S of $\{0, \ldots, d-1\}$, $\varepsilon_{d,S}$ denotes the element of E given as $\varepsilon_{d,S} = \prod_{i=0}^{(l/d)-1} \prod_{j \in S} \varepsilon_{id+j}$.

In the following four subsections automorphism groups of graphs in each of the four families of edge-transitive rose window graphs are determined.

4.3.1 Family (a)

Let Γ be the edge-transitive rose window graph $R_n(2,1)$ belonging to family (a). Then Γ can be written as the lexicographical product (also called the wreath product) $C_n[K_2^c]$ of the n-cycle C_n with the empty graph K_2^c on two vertices. It is well known that with the exception of $\Gamma = R_4(2,1) = K_{4,4}$, in which case $\mathrm{Aut}(\Gamma) = \mathbb{Z}_2 \wr S_4$ is of order $|\mathrm{Aut}(\Gamma)| = 2(4!)^2$, the automorphism group $\mathrm{Aut}(\Gamma)$ of Γ is the wreath product $D_n \wr S_2$. For an explicit description consider the partition of $V(\Gamma)$ into the sets $\{x_i, y_{i-1}\}$, $i \in \mathbb{Z}_n$. This partition is $\mathrm{Aut}(\Gamma)$-invariant, and the kernel of $\mathrm{Aut}(\Gamma)$ acting on the corresponding classes is generated by the involutions $\varepsilon_i = (x_i,\, y_{i-1})$, where $i \in \mathbb{Z}_n$. Let $E = \langle \varepsilon_0, \ldots, \varepsilon_{n-1} \rangle$. Then clearly, E is normal in $\mathrm{Aut}(\Gamma)$, $E \cong \mathbb{Z}_2^n$, and $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(W_n) = E \rtimes \langle \rho, \mu \rangle$.

4.3.2 Family (b)

Let $n = 2m$ and let $\Gamma = R_{2m}(m+2, m+1)$ be the edge-transitive rose window graph which is isomorphic to the graph $R_{2m}(m-2, m-1)$ in family (b). In [47] the automorphism group $\mathrm{Aut}(\Gamma)$ is obtained as follows. It is proved that the partition of $V(\Gamma)$ into the sets $\{x_i, x_{i+m}, y_{i-1}, y_{i-1+m}\}$, $i \in \{0, \ldots, m-1\}$, is an $\mathrm{Aut}(\Gamma)$-invariant partition and that the corresponding kernel of $\mathrm{Aut}(\Gamma)$ acting on these partition sets is generated by involutions $\varepsilon_i = (x_i, y_{i-1})(x_{i+m}, y_{i-1+m})(x_{i+1}, y_{i+m})(x_{i+1+m}, y_i)$, $i \in \{0, \ldots, m-1\}$. Let $E = \langle \varepsilon_0, \ldots, \varepsilon_{m-1} \rangle$. Then, it can be seen that $E \cong \mathbb{Z}_2^m$ and $\mathrm{Aut}(\Gamma) = E \rtimes \langle \rho\varepsilon_0, \mu\rho^m \rangle \cong \mathbb{Z}_2^m \rtimes D_m$.

4.3.3 Family (c)

Throughout this subsection let $n = 12m$ and let Γ be the edge-transitive

rose window graph $R_{12m}(3d+2, 9d+1)$, where $d = m$ or $-m$, that is, $\Gamma = R_{12m}(3m+2, 9m+1)\} = R_{12m}(3m+2, 3m-1)$ or $\Gamma = R_{12m}(9m+2, 3m+1) \cong R_{12m}(3m-2, 3m+1)$, respectively. Define the permutation σ of $V(\Gamma)$ by

$$x_i^\sigma = \begin{cases} x_i & \text{if } i \equiv 0 \pmod 3 \\ y_{i-1} & \text{if } i \equiv 1 \pmod 3 \\ y_{i+1-a} & \text{if } i \equiv 2 \pmod 3 \end{cases} \quad \text{and} \quad y_i^\sigma = \begin{cases} x_{1+i} & \text{if } i \equiv 0 \pmod 3 \\ x_{i-1+a} & \text{if } i \equiv 1 \pmod 3 \\ y_{i+6d} & \text{if } i \equiv 2 \pmod 3 \end{cases},$$

and if $m \equiv 2 \pmod 4$ then define τ by

$$x_i^\tau = \begin{cases} x_{bi} & \text{if } i \equiv 0 \pmod 3 \\ y_{bi-b} & \text{if } i \equiv 1 \pmod 3 \\ x_{b+bi-1} & \text{if } i \equiv 2 \pmod 3 \end{cases} \quad \text{and} \quad y_i^\tau = \begin{cases} x_{1+bi} & \text{if } i \equiv 0 \pmod 3 \\ y_{4+bi-4b} & \text{if } i \equiv 1 \pmod 3 \\ y_{b+bi-1} & \text{if } i \equiv 2 \pmod 3 \end{cases},$$

where $b = d+1$. (Note that $a = 3b-1$, $r = 4-3b$ and $3b^2 \equiv 3 \pmod{12m}$.) It was shown in [47] that $\sigma \in \mathrm{Aut}(\Gamma)$, and if $m \equiv 2 \pmod 4$ then also $\tau \in \mathrm{Aut}(\Gamma)$. We will show that $\mathrm{Aut}(\Gamma) = \langle \rho, \mu, \sigma, \tau \rangle$ when $m \equiv 2 \pmod 4$ and $\mathrm{Aut}(\Gamma) = \langle \rho, \mu, \sigma \rangle$ otherwise (see Proposition 4.3.4). The following lemmas are needed in this respect.

Lemma 4.3.1. *Let $H = \langle \rho^{3m} \rangle$. Then the orbits of H form an $\mathrm{Aut}(\Gamma)$-invariant partition.*

Proof. If $m \leq 4$, then one can calculate directly, we used the package MAGMA [11], that H is normal in $\mathrm{Aut}(\Gamma)$, which implies the lemma. Thus below we assume that $m > 4$. Let Π be the partition of $V(\Gamma)$ into the orbits of H and let Γ^2 denote the distance-2-graph of Γ, that is, the graph with the same vertex set as Γ, and $u \sim v$ in Γ^2 if and only if $d_\Gamma(u, v) = 2$. Let $S_i = \{x_{3lm+i+1}, y_{3lm+i} \mid l \in \{0, 1, 2, 3\}\}$, where $i \in \{0, \ldots, 3m-1\}$, see the local picture of the graph drawn in Figure 4.2 below.

First, observe that $\Gamma^2[S_i] = K_{4,4}$ for each $i \in \{0, \ldots, 3m-1\}$. The partition of $V(\Gamma^2)$ into the bipartition sets of all $\Gamma^2[S_i]$ is equal to Π. We complete the proof by showing that if $S \subset V(\Gamma^2)$ such that $\Gamma^2[S] = K_{4,4}$, then $S = S_i$ for some $i \in \{0, \ldots, 3m-1\}$. Because of this Π is $\mathrm{Aut}(\Gamma^2)$-invariant, and hence $\mathrm{Aut}(\Gamma)$-invariant as well.

Let $S \subset V(\Gamma^2)$ such that $\Gamma^2[S] = K_{4,4}$. We see that Γ^2 has degree 12, and a vertex $u \in S_i$ has exactly 2 neighbors from each H-orbit contained in both S_{i-2} and S_{i+2}, and exactly 4 from S_i. Using this and that $m > 4$ we find that for $i, j \in \{0, \ldots, 3m-1\}$, if two vertices $u \in S_i$ and $v \in S_j$ share more than 2 pairwise nonadjacent neighbors in Γ^2, then $|i-j| = 2$. Thus

$$S \subset S_i \cup S_{i+2} \text{ for some } i \in \{0, \ldots, 3m-1\}.$$

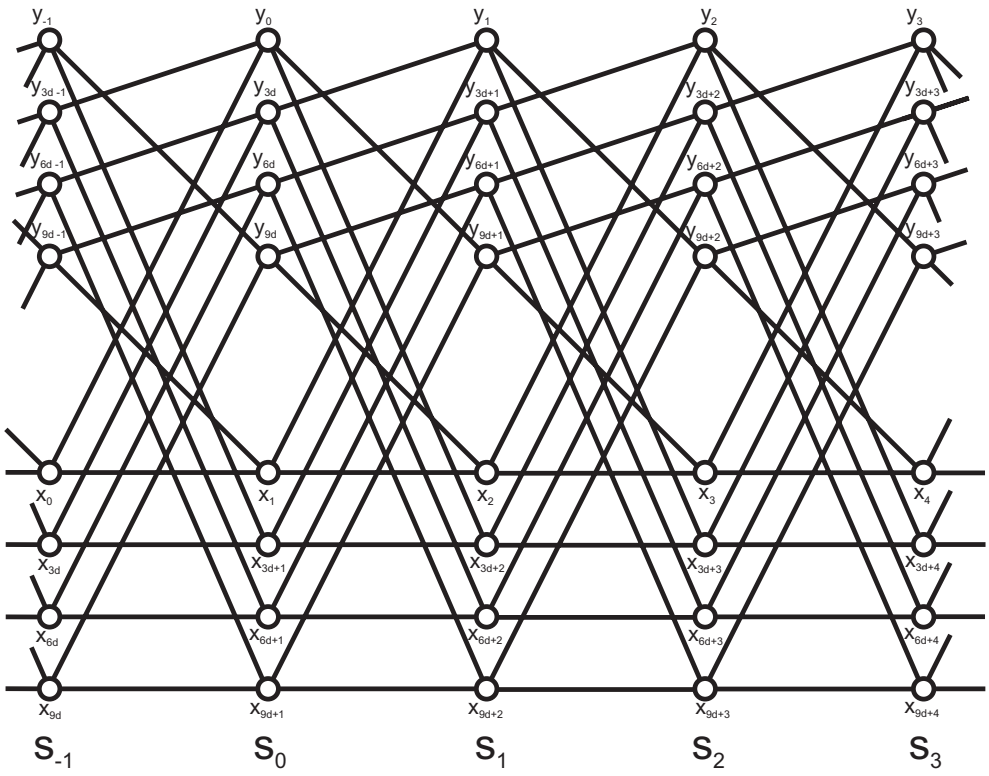

Figure 4.2: The rose window graph $\Gamma = R_{12m}(3d+2, 9d+1)$, where $d = m$ or $-m$.

Now choose two vertices u and v in S from the same H-orbit. Let $w_1, \ldots, w_k$ be those vertices in S which belong to the same H-orbit, and are adjacent to both u and v in Γ^2. It can be checked directly (see Figure 4.2) that $k > 1$ forces that

$$\{u, v, w_1, \ldots, w_k\} \subset S_j, \text{ where } j \in \{i, i+2\}.$$

Using this observation it is not hard to show that either $S = S_i$ or $S = S_{i+2}$, and by this the proof is completed.

Clearly, the subgroup H, given in Lemma 4.3.1, is of order 4, and it acts semiregularly on the vertex set $V(\Gamma)$. In addition, the corresponding quotient graph belongs to family (a), in particular $\Gamma/H = R_{3m}(2, 1) = W_{3m}$, and since, by Lemma 4.3.1, the orbits of H form an $\mathrm{Aut}(\Gamma)$-invariant partition, the whole automorphism group $\mathrm{Aut}(\Gamma)$ of Γ projects to a subgroup of $\mathrm{Aut}(W_{3m})$. On the other hand, the graph Γ can be viewed as an H-covering graph (that is, $\mathbb{Z}_4$-covering) of W_{3m}, and it can therefore be derived from W_{3m} through a suitable voltage assignment. To find this voltage assignment fix the spanning tree T of W_{3m} as the one consisting of the edges $x_i y_i$ and

$x_j x_{j+1}$, where $i, j \in \{0, \ldots, 3m-1\}$ and $j \neq 3m-1$ (see also Figure 4.3, where $e = 3m$). Then the required T-reduced voltage assignment ζ is given by the following lemma.

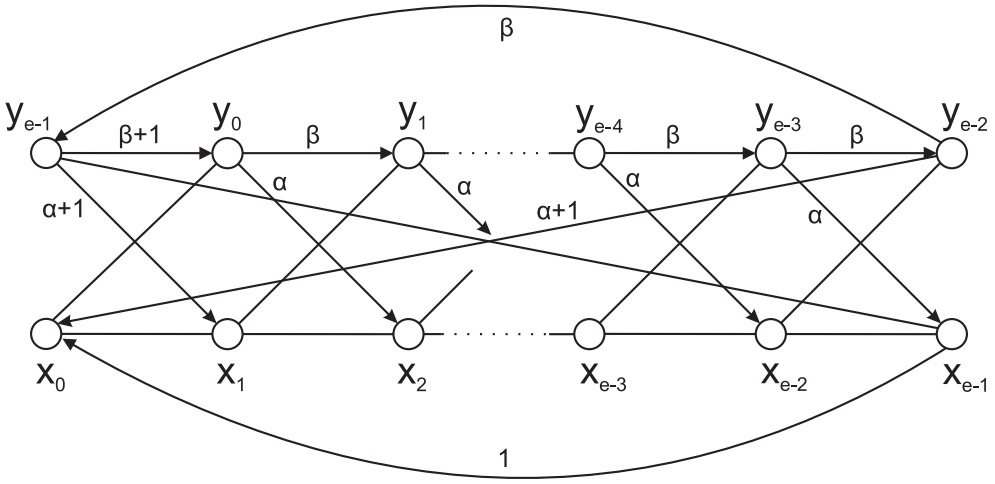

Figure 4.3: The voltage assignment ζ, where $e = 3m$.

Lemma 4.3.2. *Let $\alpha, \beta \in \mathbb{Z}_4$ be such that $(\alpha, \beta) = (1,3)$ and $(3,1)$ for, respectively, $d = m$ and $d = -m$, and let $\zeta\colon A(W_{3m}) \to \mathbb{Z}_4$ be the T-reduced voltage assignment with voltages of cotree arcs as shown in Figure 4.3. Then $W_{3m} \times_\zeta \mathbb{Z}_4 \cong \Gamma$.*

Proof. The mapping $\phi\colon V(\Gamma) \to V(W_{3m} \times_\zeta \mathbb{Z}_4)$, defined by $x^\phi_{3mj+i} = (x_i, j)$ and $y^\phi_{3mj+i} = (y_i, j)$, where $i \in \{0, 1, \ldots, 3m-1\}$ and $j \in \{0,1,2,3\}$, is an isomorphism between Γ and $W_{3m} \times_\zeta \mathbb{Z}_4$.

Lemma 4.3.3. *The largest subgroup of* $\mathrm{Aut}(W_{3m})$ *which lifts with respect to the natural projection $W_{3m} \times_\zeta \mathbb{Z}_4 \cong \Gamma \to \Gamma/H \cong W_{3m}$, where $H = \langle \rho^{3m} \rangle$ and ζ is as given in Lemma 4.3.2, is the group*

$$J = \begin{cases} \langle \rho_{W_{3m}}, \mu_{W_{3m}}, \varepsilon_{3,\{0\}} \rangle & \text{if } m \equiv 2 \pmod 4 \\ \langle \rho_{W_{3m}}, \mu_{W_{3m}}, \varepsilon_{3,\{0,1\}} \rangle & \text{otherwise} \end{cases}.$$

Proof. Recall from Subsection 4.3.1 that $\mathrm{Aut}(W_{3m}) = E \rtimes \langle \rho_{W_{3m}}, \mu_{W_{3m}} \rangle \cong \mathbb{Z}_2^{3m} \rtimes D_{3m}$ where $E = \langle \varepsilon_0, \ldots, \varepsilon_{3m-1} \rangle$. Clearly, $\rho_{W_{3m}}, \mu_{W_{3m}} \in J$. Thus to prove the lemma it is sufficient to prove that the largest subgroup of E which lifts is the group

$$F = \begin{cases} \langle \varepsilon_{3,\{0\}}, \varepsilon_{3,\{1\}}, \varepsilon_{3,\{2\}} \rangle & \text{if } m \equiv 2 \pmod 4 \\ \langle \varepsilon_{3,\{0,1\}}, \varepsilon_{3,\{1,2\}} \rangle & \text{otherwise} \end{cases}.$$

Let F' denote the largest subgroup of E which lifts. Using Proposition 4.1.4 it can be seen that $F \leq F'$. Moreover, since $\rho_{W_{3m}}, \mu_{W_{3m}} \in J$, we have that

$$\text{if } \phi \in F' \text{ then } \phi^{\rho_{W_{3m}}}, \phi^{\mu_{W_{3m}}} \in F'. \tag{4.1}$$

It is convenient to view elements ε in E as vectors in $\mathbb{Z}_2^{3m}$. Namely, we write $\varepsilon = (e_0, \ldots, e_{3m-1})$ where $e_i = 1$ if and only if ε_i actually appears in ε. Note that in this context (4.1) can be interpreted as follows: F' is invariant under the "cyclic shift" $\phi = (f_0, f_1, \ldots, f_{n-1}) \mapsto (f_{n-1}, f_0, \ldots, f_{n-2})$, and under the "reflection around the first entry" $\phi = (f_0, f_1, \ldots, f_{n-1}) \mapsto (f_0, f_{n-1}, f_{n-2}, \ldots, f_2, f_1)$.

Next we show that $\omega = \varepsilon_{3,\{0,1,2\}} = (1, \ldots, 1) \in F'$ if and only if $m \equiv 2 \pmod 4$. If $m \equiv 2 \pmod 4$, then $\omega \in F \leq F'$. On the other hand, if $\omega \in F'$ then applying Proposition 4.1.4 to the fundamental cycles $C = (x_0, y_0, y_1, x_1)$ and $C' = (x_0, x_1, \ldots, x_{3m-1})$, we get, respectively, $-\beta = \zeta(C^\omega) = \gamma\zeta(C) = \gamma\beta$ and $3m\beta + 1 = \zeta(C'^\omega) = \gamma\zeta(C') = \gamma$, where γ is an element in $\mathbb{Z}_4^*$. It follows that $3m\beta + 1 \equiv -1 \pmod 4$ and thus $m \equiv 2 \pmod 4$, as required.

Now choose $\phi \in F'$. Then there exists $\varepsilon \in F$ such that the first two components of $\psi = \phi\varepsilon$ are both equal to 1, that is, $\psi = (1, 1, \ldots)$. We complete the proof by showing that

$$\psi = \varepsilon_{3,\{0,1\}}, \text{ or } \psi = \omega \text{ and } m \equiv 2 \pmod 4. \tag{4.2}$$

Assume that the third component of ψ equals 0, that is, $\psi = (1, 1, 0, \ldots)$. Then, we claim, $\psi = (1, 1, 0, 1, \ldots)$; for if this were not the case then applying Proposition 4.1.4 to ψ with $C = (x_0, y_0, y_1, x_1)$ and $C' = (x_1, y_1, y_2, x_2)$ we get, that $-2\beta + \alpha = \zeta(C^\phi) = \zeta(C'^\phi) = 2\beta - \alpha$, which implies that $0 = 4\beta = 2\alpha = 2$, a contradiction. From this we can conclude that if $\psi \neq \varepsilon_{3,\{0,1\}}$, then applying a suitable cyclic shift to ψ we get that either $\psi' = (1, 0, 1, 0, \ldots) \in F'$ or $\psi'' = (1, 1, 1, 0, \ldots) \in F'$. But applying Proposition 4.1.4 to ψ' and ψ'' with $C = (x_0, y_0, y_1, x_1)$ and $C' = (x_1, y_1, y_2, x_2)$ we get, respectively, $\beta = \zeta(C^{\psi'}) = \zeta(C'^{\psi'}) = -\beta$ and $-\beta = \zeta(C^{\psi''}) = \zeta(C'^{\psi''}) = \alpha - 2\beta$, both are clearly impossible. It therefore follows that, if $\psi \neq \omega$, then $\psi = \varepsilon_{3,\{0,1\}}$. Thus (4.2) holds, and the proof is competed.

The following proposition proves [47, Conjecture 5] which says that a stabilizer of an arc in $\mathrm{Aut}(\Gamma)$ is of order 2 if $m \equiv 2 \pmod 4$, and of order 1 in all other cases.

Proposition 4.3.4. *Let Γ be an edge-transitive rose window graph belonging to family (c). Then $\mathrm{Aut}(\Gamma) = G$, where*

$$G = \begin{cases} \langle \rho, \mu, \sigma, \tau \rangle & \text{if } m \equiv 2 \pmod 4 \\ \langle \rho, \mu, \sigma \rangle & \text{otherwise} \end{cases}.$$

Proof. By Lemma 4.3.1, the graph Γ is a H-covering graph of the graph W_{3m}, where $H = \langle \rho^{3m} \rangle$. For $\alpha \in \mathrm{Aut}(\Gamma)$, we let $\widehat{\alpha}$ denote the projection of α into $\mathrm{Aut}(W_{3m})$, and let $\widehat{K} = \{\widehat{\alpha} \colon \alpha \in K\}$, where $K \leq \mathrm{Aut}(\Gamma)$. For example, $\widehat{\rho}_\Gamma = \rho_{W_{3m}}$ and $\widehat{\mu}_\Gamma = \mu_{W_{3m}}$. Since, by Lemma 4.3.1, the orbits of H form an $\mathrm{Aut}(\Gamma)$-invariant partition of $V(\Gamma)$ it follows that the full automorphism group $\mathrm{Aut}(\Gamma)$ of Γ project to $\mathrm{Aut}(W_{3m})$. Since the projection $\widehat{G}$ of G into $\mathrm{Aut}(W_{3m})$ is isomorphic to the group J given in Lemma 4.3.2, it follows that $\mathrm{Aut}(\Gamma) = G$.

We end this subsection by the following result which shows that another conjecture proposed by Wilson is also true (see [47, Conjecture 6]).

Theorem 4.3.5. *If m is divisible by 4 then the two graphs $R_{12m}(3m + 2, 3m - 1)$ and $R_{12m}(3m - 2, 3m + 1)$ in class (c) are isomorphic.*

Proof. Let $\Gamma = R_{12m}(3m + 2, 9m + 1) = R_{12m}(3m + 2, 3m - 1)$ and $\Gamma' = R_{12m}(9m+2, 3m+1) \cong R_{12m}(3m-2, 3m+1)$. Then, by Lemma 4.3.2, $\Gamma \cong W_{3m} \times_\zeta \mathbb{Z}_4$ and $\Gamma' \cong W_{3m} \times_{\zeta'} \mathbb{Z}_4$, where $\zeta, \zeta' \colon A(W_{3m}) \to \mathbb{Z}_4$ are T-reduced voltage assignments with voltages of cotree arcs as shown in Figure 4.3, and, respectively, $(\alpha, \beta) = (1, 3)$ and $(3, 1)$. Recall that $\omega = \varepsilon_{3,\{0,1,2\}} = \prod_{i=0}^{3m-1}(x_i, y_{i-1})$ is an automorphism of $\mathrm{Aut}(W_{3m})$. Since m is divisible by 4, we have that $\zeta(C) = \zeta'(C^\omega)$ for every fundamental cycle C with respect to the spanning tree T (see Table 4.1). Applying Proposition 4.1.5 we get that $\Gamma \cong \Gamma'$.

C	$\zeta(C)$	C^ω	$\zeta'(C^\omega)$	
$(y_{i-1}, y_i, x_i, x_{i-1})$	$\beta = 3$	$(x_i, x_{i+1}, y_{i-1}, y_{i-2})$	$-\beta = 3$	$1 \leq i \leq e-1$
$(y_{e-1}, y_0, x_0, x_1, \ldots, x_{e-1})$	$\beta + 1 = 0$	$(x_0, x_1, y_{e-1}, y_0, \ldots, y_{e-2})$	$-\beta + 1 = 0$	
$(y_{i-1}, x_{i+1}, x_i, x_{i-1})$	$\alpha = 1$	$(x_i, y_i, y_{i-1}, y_{i-2})$	$-2\beta + \alpha = 1$	$1 \leq i \leq e-2$
$(y_{e-2}, x_0, x_1, \ldots, x_{e-2})$	$\alpha + 1 = 2$	$(x_{e-1}, y_{e-1}, y_0, \ldots, y_{e-3})$	$(e-2)\beta + 1 + \alpha = 2$	
$(y_{e-1}, x_1, x_2, \ldots, x_{e-1})$	$\alpha + 1 = 2$	$(x_0, y_0, y_1, \ldots, y_{e-2})$	$(e-2)\beta + 1 + \alpha = 2$	
$(x_{e-1}, x_0, x_1, \ldots, x_{e-2})$	1	$(y_{e-2}, y_{e-1}, y_0, \ldots, y_{e-3})$	$e\beta + 1 = 1$	

Table 4.1: The voltages of fundamental cycles with respect to ζ and the voltages of their images under ω with respect to ζ', where $e = 3m$.

4.3.4 Family (d)

Throughout this subsection let $n = 2m$ and let Γ be an edge-transitive rose window graph belonging to family (d), that is, $\Gamma = R_{2m}(2b, r)$, where $2 \leq 2b \leq m$, $b^2 \equiv \pm 1 \pmod{m}$, and $r = 1$, or $r = m - 1$ and m is even. The following result about $\mathrm{Aut}(\Gamma)$ can be deduced from [33].

Proposition 4.3.6. ([33, Propositions 3.7 and 3.8]) *If* Γ *is as above but in neither of families (a) and (b), then the subgroup* $H_m = \langle \rho^2 \rangle$ *is normal in* $\mathrm{Aut}(\Gamma)$.

Define the permutation σ of $V(\Gamma)$ for $b^2 \equiv 1 \pmod{m}$ by the rule

$$x_i^\sigma = \begin{cases} x_{bi} & \text{if } i \text{ is even} \\ y_{bi-b} & \text{if } i \text{ is odd} \end{cases} \quad \text{and} \quad y_i^\sigma = \begin{cases} x_{1+bi} & \text{if } i \text{ is even} \\ y_{bi-b+r} & \text{if } i \text{ is odd} \end{cases},$$

and for $b^2 \equiv -1 \pmod{m}$ by the rule

$$x_i^\sigma = \begin{cases} x_{bi} & \text{if } i \text{ is even} \\ y_{bi-b} & \text{if } i \text{ is odd} \end{cases} \quad \text{and} \quad y_i^\sigma = \begin{cases} x_{-1+bi} & \text{if } i \text{ is even} \\ y_{bi-b-r} & \text{if } i \text{ is odd} \end{cases}.$$

It was shown in [47] that $\sigma \in \mathrm{Aut}(\Gamma)$. Let $G = \langle \rho, \mu, \sigma \rangle$. The following proposition proves [47, Conjecture 3] which says that, the stabilizer of an arc in $\mathrm{Aut}(\Gamma)$ is trivial.

Proposition 4.3.7. *If* Γ *is in neither of families (a) and (b) then* $\mathrm{Aut}(\Gamma) = G$.

Proof. Let $A = \mathrm{Aut}(\Gamma)$ and $x = x_0$. To prove that $A = G$ it is enough to show that $|A_x| \leq 4$. For this purpose let $X = \{x_i \mid i \in \mathbb{Z}_{2m} \text{ even}\}$, and let $\Gamma' = \Gamma^2[X]$, that is, $x_{2i} \sim x_{2j}$ in Γ' if and only if $d_\Gamma(x_{2i}, x_{2j}) = 2$. Note that Γ' is of degree 4 if $2 < a < n-2$, and of degree 2 otherwise. Clearly, X is an orbit of H_m in $V(\Gamma)$. By Proposition 4.3.6, H_m is normal in $\mathrm{Aut}(\Gamma)$. It follows that H_m and A_x leave X invariant. Let H_m^X and A_x^X be constituents of H_m and A_x, respectively.

Then one can see that the following properties hold:

1. $H_m \cong H_m^X \leq \mathrm{Aut}(\Gamma')$, and H_m^X is regular on $X = V(\Gamma')$.
2. A_x^X normalizes H_m^X (since H_m is normal in A).
3. $A_x^X \leq \mathrm{Aut}(\Gamma')$.

Let $P = A_x^X$. The first two properties show that P is permutation isomorphic to a subgroup of the holomorph $\mathrm{Hol}(H_m)$ (see [19]). Further, every element $\pi \in P$ can be associated with a number $k \in \{1, \ldots, m-1\}$, $\gcd(k, m) = 1$, in such a way that $x_{2i}^\pi = x_{2ik}$ for all $i \in \mathbb{Z}_m$. Thus for the vertex stabilizer P_{x_2} of $x_2 \in X$, we have that $|P_{x_2}| = 1$. Observe that $x_2 \in N_{\Gamma'}(x)$. Therefore,

$$|A_x^X| = |P| = |P_{x_2}||x_2^P| \leq |N_{\Gamma'}(x)| = \begin{cases} 4 & \text{if } 2 < a < n-2 \\ 2 & \text{otherwise.} \end{cases}$$

Let K be the kernel of A_x acting on X. To obtain that $|A_x| \leq 4$ it is enough to show that

$$|K| = \begin{cases} 1 & \text{if } 2 < a < n-2 \\ 2 & \text{otherwise.} \end{cases}$$

For this purpose let $\alpha \in K$, that is, $x_{2i}^{\alpha} = x_{2i}$ for all i. If $2 < a < n-2$ then for every $i \in \mathbb{Z}_n$ we have that $N_\Gamma(x_{2i}) \cap N_\Gamma(x_{2i+2}) = \{x_{2i+1}\}$ and $N_\Gamma(x_i) \cap N_\Gamma(x_{i+a}) = \{y_i\}$, which imply that $\alpha = 1_{A_x}$, the identity element of A_x, and thus $|K| = 1$. Now assume that $a = 2$. Since Γ is in none of families (a) and (b) we have that $r = m-1$ and that $m \geq 6$ is an even number. Observe next that the 4-cycles $(x_{2i}, x_{2i+1}, x_{2i+2}, y_{2i})$, $i \in \mathbb{Z}_n$, are fixed by α. Further, α can act on the set $\{x_1, x_3, \ldots, x_{2m-1}, y_0, y_2, \ldots, y_{2m-2}\}$ in two ways: either fixes each vertex, or switches all pairs x_{2i+1}, y_{2i}. In the former case $\alpha = 1_{A_x}$, while in the latter case we get that α also switches all pairs y_{2i+1}, y_{2i+1+m}. Therefore $|K| = 2$, and the proof is completed.

4.4 The proof of the main theorem

Throughout this section let Γ be a rose window graph and let $\mathcal{M}(\Gamma)$ be the set of all rotary maps with underlying graph Γ. If $\mathcal{M}(\Gamma) \neq \emptyset$ then clearly Γ is edge-transitive, and thus it belongs to one of the four families (a)-(d). Theorem 4.2.3 is proven after a careful analysis of each of these families in the following four subsections. In fact, Theorem 4.2.3 is a direct consequence of Propositions 4.4.4, 4.4.8, 4.4.9 and 4.4.10.

4.4.1 Family (a)

Throughout this subsection let $\Gamma = R_n(2,1)$. Recall from Subsection 4.3.1 that for $\Gamma \neq R_4(2,1)$ we have $\mathrm{Aut}(\Gamma) = E \rtimes \langle \rho, \mu \rangle \cong \mathbb{Z}_2^n \rtimes D_n$, where $E = \langle \varepsilon_0, \ldots, \varepsilon_{n-1} \rangle$.

Lemma 4.4.1. *Let Γ be different from $R_4(2,1)$, let $\mathcal{M} \in \mathcal{M}(\Gamma)$, let $T = E \cap \mathrm{Aut}(\mathcal{M})$, let $\phi = (t_j)_{j \in \mathbb{Z}_n}$ and $\phi' = (t'_j)_{j \in \mathbb{Z}_n}$ be any two elements in T, and let $i \in \mathbb{Z}_n$. Then the following hold:*

$$|T| = 8, T^\rho = T, T^\mu = T, \text{ and if } t_i = t'_i,\ t_{i+1} = t'_{i+1} \text{ and } t_{i+2} = t'_{i+2} \text{ then } \phi = \phi' \quad (4.3)$$

Proof. Let $K = \mathrm{Aut}(\mathcal{M})$, and denote by $F(\mathcal{M})$ the set of cycles of Γ which are the boundaries of faces of $\mathcal{M}$. As remarked in the introduction, each $X \in F(\mathcal{M})$ is a consistent cycle. By Proposition 4.1.1, $\mathrm{Aut}(\Gamma)$ has 3 orbits on the set of (directed) consistent cycles of Γ. These orbits have representatives (x_0, x_1, y_{n-1}, y_0) of length 4, $(x_0, x_1, \ldots, x_{n-1})$ of length n,

and $(x_0, x_1, \ldots, x_{n-1}, y_{n-1}, y_0, \ldots, y_{n-2})$ of length $2n$. As the sets $\{x_i, y_i\}$, $i \in \mathbb{Z}_n$, are blocks of $\mathrm{Aut}(\Gamma)$, it is not difficult to see that the consistent 4-cycles are $(x_i, x_{i+1}, y_{i-1}, y_i)$, $i \in \mathbb{Z}_n$. Therefore, each edge of Γ lies on exactly one such 4-cycle, and so the cycles in $F(\mathcal{M})$ must have length n or $2n$. Let us fix one X in $F(\mathcal{M})$, and write $|X|$ for its length. The group E acts transitively on the set $\Sigma = \{X^\alpha \mid \alpha \in \mathrm{Aut}(\Gamma)\}$. In particular, if $X = (x_0, x_1, \ldots, x_{n-1})$ then ρ and μ fix X. Since Σ is an orbit of $\mathrm{Aut}(\Gamma) = E \rtimes \langle \rho, \mu \rangle$, E must be transitive on Σ. Similarly, one can show this fact for the case when $X = (x_0, x_1, \ldots, x_{n-1}, y_{n-1}, y_0, \ldots, y_{n-2})$. Since E is abelian, the action of E/E_0 on Σ is regular, where E_0 denotes the kernel of the action. Moreover, $E_0 = 1$ if $|X| = n$, while $E_0 = \langle \omega = (1, \ldots, 1) \rangle$ if $|X| = 2n$. Let $T' = \{\varepsilon \in E \mid X^\varepsilon \in F(\mathcal{M})\}$. Clearly, $T \subseteq T'$. Since $\mathcal{M}$ is a rotary map, either each face of $\mathcal{M}$ is of length $|X| = n$ or each face of $\mathcal{M}$ is of length $|X| = 2n$. Therefore, $|E(\Gamma)| = |F(\mathcal{M})||X|/2$. It follows that $|F(\mathcal{M})| = 8$ for $|X| = n$ and $|F(\mathcal{M})| = 4$ for $|X| = 2n$. Then $|T'| = 8$ because $|T'| = |F(\mathcal{M})|$ for $|X| = n$ and $|T'| = 2|F(\mathcal{M})|$ for $|X| = 2n$. Now pick $\varepsilon \in T'$. Clearly, $\varepsilon \in K$ if and only if $\{X^{\phi\varepsilon} \mid \phi \in T'\} = F(\mathcal{M})^\varepsilon = F(\mathcal{M}) = \{X^\phi \mid \phi \in T'\}$, which is equivalent to the statement that $T'\varepsilon = T'$. Thus $T'T = T'$ which implies that T' is a subgroup of E, and so $T' \leq K$. Thus $T' = T$, that is, $|T| = 8$.

Further, observe that K contains elements of the form $\rho\varepsilon$ and $\mu\varepsilon'$, where $\varepsilon, \varepsilon' \in E$. Because of that we have $T = T^{(\varepsilon\rho^{-1})} = T^{\rho^{-1}}$ and $T = T^{(\varepsilon'\mu^{-1})} = T^{\mu^{-1}}$, and thus $T^\rho = T$ and $T^\mu = T$. Recall that $T^\rho = T$ means that T, when viewed as subspace of $\mathbb{Z}_2^n$, is invariant under cyclic shifts of vectors.

Now the lemma follows from the following implication: $\phi = (0, 0, 0, \ldots) \in T \;\Rightarrow\; \phi = (0, \ldots, 0)$. In particular, ϕ and ϕ^ρ both fix the arc (x_1, x_2), and since, by Proposition 4.1.3, the arc stabilizer $K_{(x_1,x_2)}$ is of order $|K_{(x_1,x_2)}| = 2$, it follows that $\phi^\rho = \phi$, which implies that $\phi = (0, \ldots, 0)$.

Lemma 4.4.2. *Let Γ be different from $R_4(2, 1)$. Then $\mathcal{M}(\Gamma) \neq \emptyset$ if and only if E contains a subgroup T satisfying condition (4.3).*

Proof. The implication "$\Rightarrow$" is clear by Lemma 4.4.1. For the implication "$\Leftarrow$" let $T \leq E$ satisfy condition (4.3). We check that $K = \langle T, \mu, \rho \rangle$ satisfies Proposition 4.1.3 (i)-(iii). It is easy to see that K is transitive on $A(\Gamma)$, that is, Proposition 4.1.3 (i) holds.

By Lemma 4.4.1, $|K| = |T||\langle \mu, \rho \rangle| = 16n$. The order of the vertex stabilizer K_{x_1} is 8, and the order of the edge stabilizer $K_{x_0x_1}$ is 4. The group K_{x_1} is faithful on $N_\Gamma(x_1)$. Namely, if $\phi \in K_{x_1}$ fixes $N_\Gamma(x_1)$ pointwise, then $\phi \in T$ follows. In this case $\phi = (0, 0, 0, \ldots)$, and hence, by (4.3), $\phi = (0, \ldots, 0)$. Thus K_{x_1} is dihedral, and therefore Proposition 4.1.3 (ii) holds, too.

Also, there exists $\psi \in T$ such that $\psi = (0, 0, 1, \ldots)$. Now ψ and $\mu\rho$ are distinct involutions in K, each fixing the edge x_0x_1. Thus $K_{x_0x_1}$ is dihedral of order 4. By this also Proposition 4.1.3 (iii) holds. This completes the proof of the lemma.

Lemma 4.4.3. *Let Γ be different from $R_4(2,1)$ and let $T \leq E$ satisfy condition (4.3). Then $\gcd(n, 12) > 2$, and T is one of the following two subgroups:*

$$T_1 = \langle \varepsilon_{3,\{0\}}, \varepsilon_{3,\{1\}}, \varepsilon_{3,\{2\}} \rangle \quad \textit{and } T_2 = \langle \varepsilon_{4,\{0,1\}}, \varepsilon_{4,\{1,2\}}, \varepsilon_{4,\{2,3\}} \rangle.$$

Proof. First observe that the groups T_i, $i \in \{1, 2\}$, satisfy condition (4.3). We show that T is indeed one of these two groups. After a suitable cyclic shift we find $\phi \in T$ such that $\phi = (1, 0, 0, 1, \ldots)$. (Observe that $n > 4$, since $\Gamma \neq R_4(2, 1)$.) We will see below that ϕ is determined uniquely by its next missing entry.

Assume first that $\phi = (1, 0, 0, 1, 0, \ldots)$. Then the reflection around the 4th entry maps ϕ to itself, see (4.3). Hence $\phi = (1, 0, 0, 1, 0, 0, \ldots)$. Also, the cyclic shift with 3 steps fixes ϕ. Thus $\phi = \varepsilon_{3,\{0\}}$ and it follows that $T = T_1$.

Assume now that $\phi = (1, 0, 0, 1, 1, \ldots)$. Then a direct check shows that $n \neq 5$. If $\phi = (1, 0, 0, 1, 1, 1, \ldots)$ then the reflection around the 5th entry maps ϕ to itself, and hence $\phi = (1, 0, 0, 1, 1, 1, 0, 0, \ldots)$. But then $\phi\phi^{\rho^2}$ and $\phi^{(\rho^{-1})}$ have the same entry on the $3 - 6$th places, but distinct entries on the 7th place, contradicting (4.3). If however $\phi = (1, 0, 0, 1, 1, 0, 1 \ldots)$ then the reflection around the 6th entry maps ϕ to itself, and thus $\phi = (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, \ldots)$, again contradicting (4.3) since in this case ϕ and ϕ^{ρ^3} have the same entries on the $6 - 9$th places, but distinct entries on the 5th place. It therefore follows that $\phi = (1, 0, 0, 1, 1, 0, 0, \ldots)$, and applying the cyclic shift with 4 steps implies that $\phi = \varepsilon_{4,\{0,3\}}$, and consequently $T = T_2$.

Observe that the complete bipartite graph $K_{4,4}$, that is the rose window graph $R_4(2, 1)$, is the underlying graph of a reflexible toroidal map of type $\{4, 4\}_{2,2}$ (see [41]). This fact, Proposition 4.1.3 and Lemmas 4.4.1, 4.4.2 and 4.4.3 combined together imply the following result.

Proposition 4.4.4. *Let Γ be a rose window graph $R_n(2, 1)$ belonging to family (a). Then $\mathcal{M}(\Gamma) \neq \emptyset$ if and only if $\gcd(n, 12) > 2$ and every $\mathcal{M} \in \mathcal{M}(\Gamma)$ is reflexible.*

4.4.2 Family (b)

Throughout this subsection let $n = 2m$, and let Γ be the rose window graph $R_{2m}(m+2, m+1)$ which is isomorphic to $R_{2m}(m-2, m-1)$ belonging

to family (b). Recall from Subsection 4.3.2 that $\mathrm{Aut}(\Gamma) = E \rtimes \langle \rho\sigma_0, \mu\rho^m \rangle \cong \mathbb{Z}_2^m \rtimes D_m$, where $E = \langle \varepsilon_0, \ldots, \varepsilon_{m-1} \rangle$.

The following two lemmas are counterparts to Lemma 4.4.1 and Lemma 4.4.2, respectively. The proofs are left to the reader.

Lemma 4.4.5. *Let $\mathcal{M} \in \mathcal{M}(\Gamma)$, let $T = E \cap \mathrm{Aut}(\mathcal{M})$, let $\phi = (t_j)_{j \in \mathbb{Z}_n}$ and $\phi' = (t'_j)_{j \in \mathbb{Z}_n}$ be any two elements in T, and let $i \in \mathbb{Z}_n$. Then the following hold:*

$|T| = 16, T^\rho = T, T^\mu = T$, *and if* $t_i = t'_i$, $t_{i+1} = t'_{i+1}$, $t_{i+2} = t'_{i+2}$ *and* $t_{i+3} = t'_{i+3}$ *then* $\phi = \phi'$ (4.4)

Lemma 4.4.6. *$\mathcal{M}(\Gamma) \neq \emptyset$ if and only if E contains a subgroup satisfying condition (4.4).*

Lemma 4.4.7. *Let $T \leq E$ satisfy condition (4.4). Then* $\gcd(m, 60) > 3$, *and T is one of the following four subgroups: $T_1 = \langle \varepsilon_{4,\{0\}}, \varepsilon_{4,\{1\}}, \varepsilon_{4,\{2\}}, \varepsilon_{4,\{3\}} \rangle$, $T_2 = \langle \varepsilon_{5,\{0,1\}}, \varepsilon_{5,\{1,2\}}, \varepsilon_{5,\{2,3\}}, \varepsilon_{5,\{3,4\}} \rangle$, $T_3 = \langle \varepsilon_{6,\{0,2\}}, \varepsilon_{6,\{1,3\}}, \varepsilon_{6,\{2,4\}}, \varepsilon_{6,\{3,5\}} \rangle$ and $T_4 = \langle \varepsilon_{6,\{0,1,2\}}, \varepsilon_{6,\{1,2,3\}}, \varepsilon_{6,\{2,3,4\}}, \varepsilon_{6,\{3,4,5\}} \rangle$.*

Proof. First observe that the groups T_i, $i \in \{1, 2, 3, 4\}$, satisfy condition (4.4). We show that T is indeed one of these groups. After a suitable cyclic shift we find $\phi \in T$ such that $\phi = (1, 0, 0, 0, 1, \ldots)$. If $m \leq 6$, then a direct check shows that $m = 5$ and $T = T_2$. Let $m > 6$. We will see below that ϕ is determined uniquely by its next two missing entries.

Assume first that $\phi = (1, 0, 0, 0, 1, 0, 0, \ldots)$. Reflecting around the 5th entry maps ϕ to itself. Thus $\phi = (1, 0, 0, 0, 1, 0, 0, 0, \ldots)$. Since the cyclic shift with 4 steps fixes ϕ we get that $\phi = \varepsilon_{4,\{0\}}$, which implies that $T = T_1$. Second, assume that $\phi = (1, 0, 0, 0, 1, 1, 0, \ldots)$. Then reflecting around the 3th entry fixes ϕ. Thus we get $\psi = \phi^{\rho^2} = (0, 1, 1, 0, 0, 0, 1, 1, 0, \ldots) \in T$. (Observe that $\phi = (1, 0, 0, 0, 1, 1, 0, 1)$ can be excluded by a direct check.) Thus ψ is fixed by a cyclic shift with 5 steps, so $\psi = \varepsilon_{5,\{1,2\}}$. It follows $T = T_2$. Third, assume that $\phi = (1, 0, 0, 0, 1, 0, 1, \ldots)$. Then again reflecting around the 3th entry fixes ϕ, hence $\psi = (t_i)_{i \in \mathbb{Z}_m} = \phi^{\rho^2} = (1, 0, 1, 0, 0, 0, 1, 0, 1, \ldots) \in T$. (Observe that $\psi = (1, 0, 0, 0, 1, 0, 1, 0)$ can be excluded by a direct check.) We show that the cyclic shift with 6 steps fixes ψ. This then implies that $\psi = \varepsilon_{6,\{0,2\}}$, and consequently $T = T_3$. For this purpose suppose that $\psi = (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, \ldots)$. Then $\psi\psi^{\rho^5}$ has entry 1 in five consecutive places, hence $\psi\psi^{\rho^5} = (1, \ldots, 1)$. It can be checked that $\psi \neq (1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$, hence $\psi = (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, \ldots)$. Now $\psi\psi^{\rho^3} = (f_{m-1}, f_{m-2}, f_{m-3}, 1, 0, 1, 1, 0, 1, 0, 1, \ldots)$, and $\psi^{\rho^{-3}} = (0, 0, 0, 1, 0, 1, 1, 1, \ldots)$. They have the same entry on the $4 - 7$th places, but differ in the 8th place, a contradiction. Finally, assume that $\phi = (1, 0, 0, 0, 1, 1, 1, \ldots)$. Then $\phi \neq (1, 0, 0, 0, 1, 1, 1)$ and $\phi \neq (1, 0, 0, 0, 1, 1, 1, 1)$. Reflecting around the 3th entry again fixes ϕ, hence $\psi = \phi^{\rho^2} = (1, 1, 1, 0, 0, 0, 1, 1, 1, \ldots) \in T$. Then $\psi\psi^3 = (1, \ldots, 1)$. Thus $\psi = \varepsilon_{6,\{0,1,2\}}$, and consequently $T = T_4$.

Lemmas 4.4.5, 4.4.6 and 4.4.7 combined together imply the following result.

Proposition 4.4.8. *Let Γ be a rose window graph $R_{2m}(m-2, m-1)$ belonging to family (b). Then $\mathcal{M}(\Gamma) \neq \emptyset$ if and only if $\gcd(m, 60) > 3$ and every $\mathcal{M} \in \mathcal{M}(\Gamma)$ is reflexible.*

4.4.3 Family (c)

Let $n = 12m$. Then a rose window graph belonging to family (c) is isomorphic to the graph $\Gamma = R_{12m}(3d+2, 9d+1)$, where $d = m$ or $-m$. Recall from Subsection 4.3.3 that

$$\mathrm{Aut}(\Gamma) = G = \begin{cases} \langle \rho, \mu, \sigma, \tau \rangle & \text{if } m \equiv 2 \pmod 4 \\ \langle \rho, \mu, \sigma \rangle & \text{otherwise} \end{cases}.$$

In addition, if $m \equiv 2 \pmod 4$ then $|G| = 2|A(\Gamma)|$, $G_{x_0} = \langle \mu, \tau \rangle \cong D_4$, $\tau\mu$ permutates $N_\Gamma(x_0)$ in a 4-cycle, and $G_{x_0x_1} = \langle \mu\rho, \mu\tau\mu \rangle \cong D_2$. On the other hand if $m \not\equiv 2 \pmod 4$ then $|G| = |A(\Gamma)|$, and $G_{x_0} = \langle \mu, \sigma \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. All these combined together with Propositions 4.1.2 and 4.1.3 imply the following result.

Proposition 4.4.9. *Let Γ be a rose window graph belonging to family (c). Then $\mathcal{M}(\Gamma) \neq \emptyset$ if and only if $m \equiv 2 \pmod 4$ and every $\mathcal{M} \in \mathcal{M}(\Gamma)$ is reflexible.*

4.4.4 Family (d)

Let $\Gamma = R_{2m}(2b, r)$ where $b^2 \equiv \pm 1 \pmod m$, $2 \leq 2b \leq m$, and $r = 1$, or $r = m-1$ and m is even. Recall from Subsection 4.3.4 that, if Γ is in none of families (a) and (b), then $\mathrm{Aut}(\Gamma) = G = \langle \rho, \mu, \sigma \rangle$. Moreover, $|G| = |A(\Gamma)|$, and if $b^2 \equiv 1 \pmod m$ then $G_{x_0} = \langle \mu, \sigma \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. On the other hand, if $b^2 \equiv -1 \pmod m$ then $G_{x_0} = \langle \sigma \rangle \cong \mathbb{Z}_4$. All these combined together with Propositions 4.1.2 and 4.1.3 imply the following result.

Proposition 4.4.10. *Let Γ be a rose window graph $R_{2m}(2b, r)$ belonging to family (d) which is in none of families (a) and (b). Then $\mathcal{M}(\Gamma) \neq \emptyset$ if and only if $b^2 \equiv -1 \pmod m$ and every $\mathcal{M} \in \mathcal{M}(\Gamma)$ is chiral.*

4.4.5 Proof of the main theorem

Results of previous four subsections the proof of the main theorem is now at hand.

PROOF OF THEOREM 4.2.3: Let $\Gamma = R_n(a, r)$ be a rose window graph underlying a rotary map $\mathcal{M}$, $1 \leq a, r \leq n/2$. Then Γ is edge-transitive and thus it belongs to one of the four families (a)-(d) stated in [33]. Propositions 4.4.4, 4.4.8, 4.4.9 and 4.4.10 combined together imply the theorem. ■

Chapter 5

Summary / Összefoglalás

5.1 Summary

The notion of *semi quadratic sets* was introduced by F. Buekenhout in 1973 [12]. Since that time a lot of attempts were made to classify all semi quadratic sets, but the problem is still open in general.

In the first section of Section 1.1 we summarize some results on semi quadratic sets. Because of the huge diversity of these objects in our researches we restrict ourselves to the planar case and we study *semiovals*. A semioval in a projective plane is a non-empty pointset S with the property that for every point in S there exists a unique tangent line passing through the point. The classical examples of semiovals arise from polarities (ovals and unitals), and from the theory of blocking sets. The study of semiovals is also motivated by their applications to cryptography [4].

For planes of small order the complete spectrum of the sizes and the number of projectively non-isomorphic semiovals are known. For $q \leq 13$ we give the complete description in $\mathrm{PG}(2, q)$.

The main aim of the first two chapters is to characterize the semiovals which are contained in the union of at most three lines. After presenting some older results on semiovals with long secants [20] and on the bounds on the size of a semioval we prove that if the semioval is contained in the union of three lines, then there are much better bounds on its size (Theorem 1.2.2).

The case when the semioval is contained in less then three lines is easy. After this we have to distinguish two different cases. In the first chapter we completely characterize the semiovals which are contained in three non-concurrent lines (Section 1.3). We use basic additive group theory, results on difference sets and combinatorial arguments.

At the end of Chapter 1 we introduce a possible generalization for the concept of semiovals and cite some known results on them (Theorem 1.4.2).

In Chapter 2 we study semiovals contained in three concurrent lines. This case is much more complicated than the previous one, here we have to introduce the concept of *strong semiovals*. There is only one infinite family of this type of semiovals arising from Baer subplanes of $\mathrm{PG}(2,q)$, where q is an even power of a prime. In Section 2.2 we give an improved upper bound for the size of semiovals in Π_q (see Theorem 2.2.2), and show that this bound is sharp (see Example 2.2.3). In Section 2.3 we give an algebraic description of semiovals in $\mathrm{PG}(2,q)$.

Finally, Section 2.4 is devoted to the study of strong semiovals. We present some necessary conditions for the existence of such objects and give a complete classification of strong semiovals in $\mathrm{PG}(2,p)$ and $\mathrm{PG}(2,p^2)$, p an odd prime.

These results motivates our final conjecture on the non-existence of strong semiovals different from the above mentioned type.

The (Δ, D)-*problem* (or *degree/diameter problem*) is to determine the largest possible number of vertices of a graph which has maximum degree Δ and diameter D. In Chapter 3 we restrict our attention to the class of *linear Cayley graphs*. After the preliminary materials we present some constructions where the resulting graphs improve the previously known, general lower bounds for vertex-transitive graphs ((3.2) and (3.3)). For small number of vertices these are also compared to the known largest vertex transitive graphs having the same degree and diameter.

It turns out that the problem for our case is to look for special pointsets in projective spaces, namely *saturating sets*. We give a short overview of the used geometric background. The graphs in our constructions arise from *comlete arcs, caps* and other objects of finite projective spaces.

In Chapter 4 we study a special class of tetravalent graphs. The concept of *rose window graphs* was introduced by Wilson in [41, 47].

Wilson was primarily interested in embeddings of graphs $R_n(a,r)$ into closed surfaces as *rotary maps*. He gave several examples of such maps, and concluded his paper [47] by a conjecture that the list of parameters n, a, r given there is the complete list of parameters giving rose window graphs which underlie rotary maps. A *map* $\mathcal{M}$ is an embedding of a finite connected graph Γ into a surface so that it divides the surface into simply-connected regions, called the *faces* of $\mathcal{M}$. The preliminary results are detailed in Section 4.1.1.

An *automorphism* of $\mathcal{M}$ is an automorphism of Γ which preserves its faces. Following [48], $\mathcal{M}$ is called *rotary* if it admits automorphisms R and S with the property that R cyclically permutes the consecutive edges of a face f, and S cyclically permutes the consecutive edges incident to some vertex v of f. In this case the automorphism group $\mathrm{Aut}(\mathcal{M})$ of $\mathcal{M}$ acts transitively on the vertex set, edge set, and face set. [6, 14, 38].

If a rotary map also contains an automorphism T which 'flips' an edge e of f, and preserves f, then we say that $\mathcal{M}$ is *reflexible*. On the other hand, if no such automorphism T exists, then $\mathcal{M}$ is called *chiral*. One of the central questions regarding maps is the following: which graphs admit an embedding onto some closed surface as a rotary map [7].

Wilson actually posed three questions about rose window graphs in [47]. Given natural numbers $n \geq 3$ and $1 \leq a, r \leq n-1$, for which n, a and r is $R_n(a, r)$ edge-transitive; when $R_n(a, r)$ is edge-transitive, what is the order of its automorphism group and for which parameters the underlying graph of a rotary map?

The first question was answered by Kovács, Kutnar and Marušič in [33], the second and third questions are discussed in Chapter 4. We use some well known results about *coverings* and *embeddings* of graphs. The basic facts on these concepts and the tools we use are also presented in the 4.1.2 subsection. A combinatorial description of a K-covering was introduced through a voltage graph by Gross and Tucker [25]. The problem of determining whether an automorphism α of Γ lifts or not is expressed in terms of voltages and we use these results as a main tool in the study of edge-transitive rose window graphs. Four families of rose window graphs are distinguished and discussed consecutively in 4.3 the automorphism groups are also determined in all cases. Finally in 4.4 our main theorem 4.2.3 which answers the third question of Wilson is proven after a careful analysis of four families of rose window graphs.

In Chapter 5 a short summary is given both in english and hungarian.

The dissertation ends with the list of references.

5.2 Összefoglalás

A *szemikvadratikus halmazok* fogalmát F. Buekenhout vezette be 1973-ban [12]. Azóta sok próbálkozás történt az osztályozásukra, de az általános probléma még nem megoldott.

Az 1.1 részben először néhány, a szemikvadratikus halmazokra vonatkozó eredményt ismertetünk. A szemikvadratikus halmazok sokfélesége miatt kutatásainkban a síkbeli esetre korlátoztuk magunkat és az ún. *szemioválisokat* tanulmányoztuk. Egy projektív síkon *szemioválisnak* nevezünk egy S nemüres ponthalmazt, ha minden P pontján keresztül pontosan egy olyan t_P egyenes létezik, amire $S \cap t_P = \{P\}$. Ezt az egyenest az S P-beli érintőjének nevezzük. A klasszikus példák szemioválisokra a polaritások (oválisok és unitálok) közül, továbbá a blokkoló halmazok köréből (csúcsnélküli háromszög) származtathatók. A szemioválisok tanulmányozását a kriptográfiai alkalmazásaik is motiválják [4].

Kis rendű síkok esetén a méretek teljes spektruma és a projektíven nem izomorf szemioválisok száma egyaránt ismert.

Az első két fejezetben azon szemioválisok karakterizációját tűztük ki célul, amelyeket három vagy annál kevesebb egyenes uniója tartalmaz. Néhány régebbi, hosszú szelőkkel rendelkező szemioválisokra vonatkozó eredmény [20] és a szemiovális méretére vonatkozó korlátok bemutatása után bebizonyítjuk, hogy az általunk vizsgált esetben jobb korlátok érvényesek (1.2.2 Tétel).

Az az eset, amikor a szemioválist már háromnál kevesebb egyenes is tartalmazza, egyszerűen kezelhető. Ezek után két különböző esetre bontjuk a vizsgálatot. Az első fejezetben arra adunk teljes karakterizációt, amikor a szemioválist tartalmazó három egyenes nem illeszkedik egy pontra (1.3 Tétel). Kombinatorikai jellegű állításokat és egyszerű eredményeket használunk az additív csoportelmélet illetve a differencia halmazok elméletének köréből.

Az első fejezet végén a szemiovális fogalom egy lehetséges általánosításáról esik szó, néhány ezekre vonatkozó eredményt is ismertetünk (1.4.2 Tétel).

A második fejezetben a másik esetet tárgyaljuk, amikor a három egyenes egy ponton megy át. Ez jóval bonyolultabb mint az előző, be kell vezetnünk a *szabályos szemioválisok* fogalmát. Csak egy végtelen osztályát ismerjük az ilyen típusú szemioválisoknak, amik $\mathrm{PG}(2,q)$ Baer részsíkjainak segítségével származtathatók ha q páros kitevőjű prímhatvány. A 2.2 részben a Π_q sík szemioválisainak méretére vonatkozó felső korláton javítunk (2.2.2 Tétel) és a 2.2.3 Példával megmutatjuk a korlát élességét. A 2.3 részben a $\mathrm{PG}(2,q)$-beli szemioválisok egy algebrai leírását adjuk.

Végül a 2.4 részben a szabályos szemioválisokat tanulmányozzuk. Szük-

séges feltételeket mutatunk szabályos szemioválisok létezésére, és prím illetve prímnégyzet rendű, testre épített síkok esetén megadjuk a teljes leírásukat (páratlan prím esetén).

Ezek az eredmények motiválják utolsó sejtésünket, hogy a fenti típuson kívül nincsenek szabályos szemioválisok.

A (Δ, D)-*probléma* (vagy *fokszám/átmérő probléma*) azon legnagyobb egész szám meghatározása, ahány csúcsú gráf létezik az adott Δ maximális fokszámú és D átmérőjű gráfok között. A harmadik fejezetben a *lineáris Cayley gráfok* körében tárgyaljuk a problémát. Az előzmények ismertetése után olyan konstrukciókat mutatunk, ahol a kapott gráfok javítanak az eddig ismert, csúcstranzitív gráfokra vonatkozó általános alsó korláton ((3.2) és (3.3)). Kis csúcsszám esetén a kapott gráfokat összehasonlítjuk a csúcstranzitív esetben ismert legnagyobb, ugyanazon paraméterekkel rendelkező gráfokkal.

Kiderül, hogy a mi esetünkben a probléma tulajdonképpen a projektív tér ún. *szaturáló halmazainak* keresését jelenti. Röviden áttekintjük a felhasznált geometriai hátteret. A konstruált gráfok *teljes ívekből, süvegekből* és a projektív tér egyéb ismert objektumaiból származtathatók.

A negyedik fejezetben a 4-reguláris gráfok egy speciális osztályát tanulmányozzuk. A *rózsaablak gráfok* fogalmát Wilson vezette be [41, 47].

Wilsont eredetileg az $R_n(a, r)$ rózsaablak gráfok zárt felületekbe való ún. *forgásszimmetrikus térképként* (*rotary map*) történő beágyazásai érdekelték. Számos példát adott ilyen térképekre és a [47] cikkét azzal a sejtéssel zárta, hogy az ott megadott, azon n, a, r paraméterekre vonatkozó listája, ami felsorolja az összes forgásszimmetrikus térképpel rendelkező rózsaablak gráfot, teljes. Egy Γ véges, összefüggő gráf, valamely felületbe történő olyan $\mathcal{M}$ beágyazásait nevezzük *térképnek* (*map*), melyek a felületet egyszeresen összefüggő tartományokra, ún. *lapokra* osztják. Az ezekre vonatkozó előzmények részleteit tartalmazza a 4.1.1 rész.

Az $\mathcal{M}$ térkép egy *automorfizmusa* alatt a Γ gráf olyan automorfizmusát értjük, ami megőrzi a lapokat. A [48] cikk elnevezéseit követve $\mathcal{M}$ térkép *forgásszimmetrikus*, ha vannak olyan R and S automorfizmusok, amik rendelkeznek azzal a tulajdonsággal, hogy R egy f lap egymást követő éleit, míg S a lap egy v csúcsának szomszédait permutálják ciklikusan. Ebben az esetben az $\mathcal{M}$ térkép $\mathrm{Aut}(\mathcal{M})$ automorfizmus-csoportja tranzitíven hat a csúcsok, az élek és a lapok halmazán is [6, 14, 38].

Ha a forgásszimmetrikus térképnek van ezeken túl olyan T automorfizmusa is, ami az f lap egy e élét mintegy megfordítja, úgy, hogy a lapot közben megőrzi, akkor a térképet *reflexibilisnek* nevezzük. Ha nincs ilyen T, akkor pedig *királisnak* hívjuk. A térképekre vonatkozó egyik központi kérdés, hogy mely gráfoknak van bizonyos zárt felületre forgásszimmetrikus térképként történő beágyazása [7].

Wilson három, a rózsaablak gráfokra vonatkozó kérdést fogalmazott meg a [47] cikkben. Milyen n, a és r paraméterek ($n \geq 3$, $1 \leq a, r \leq n-1$) esetén lesz az $R_n(a,r)$ rózsaablak gráf éltranzitv; ha $R_n(a,r)$ éltranzitív, mi az automorfizmus-csoportjának rendje és végül milyen paraméterekre lesz a gráfnak forgásszimmetrikus térképe?

Az első kérdést Kovács, Kutnar és Marušič megválaszolták [33], az értekezés negyedik fejezete pedig a második és a harmadik kérdést tárgyalja. Gráfok *fedéseire* és *beágyazásokra* vonatkozó, jól ismert eredményeket használunk fel. Ezen fogalmakkal kapcsolatos alapvető tényeket és a felhasznált eszközöket mutatja be a 4.1.2 rész. Az ún. *reguláris fedések* kombinatorikus leírását Gross és Tucker megadták a feszültség gráfok (voltage graph) fogalmát felhasználva [25]. A kérdést, hogy egy Γ gráf egy α automorfizmusa felemelhető vagy sem feszültségek segítségével is megfogalmazhatjuk. Az erre vonatkozó eredmények szolgálnak fő eszközül az éltranzitív rózsaablak gráfok tanulmányozásánál. A 4.3 részben rózsaablak gráfok négy speciális osztályát vizsgáljuk meg és minden esetben meghatározzuk az automorfizmus-csoportokat is. Végül a 4.4 részben a fő eredményünket bizonyítjuk (4.2.3 Tétel) négy eset aprólékos vizsgálatával, megválaszolva Wilson harmadik kérdését is.

Az ötödik fejezetben a dolgozat rövid angol és magyar nyelvű összefoglalását adjuk.

Az értekezés a hivatkozások felsorolásával zárul.

Bibliography

[1] Alperin, J. L. and Bell, R. B.: *Groups and Representations,* volume 162 of Graduate Texts in Mathematics, Springer Verlag, 1995.

[2] Araujo, G., Noy, M. and Serra, O.: *A geometric construction of large vertex transitive graphs of diameter two,* J. Combin. Math. Combin. Comput. **57** (2006), 97–102.

[3] Bannai, E. and Ito, T.: *On finite Moore graphs,* J. Fac. Sci. Tokyo Univ. **20** (1973), 191–208.

[4] Batten, L. M.:*Determining sets,* Australas. J. Combin. **22** (2000), 167–176.

[5] Baumert, L. D.: *Cyclic difference sets,* Lecture notes in Mathematics 182, Springer, Berlin-Heidelberg-New York, 1971.

[6] Biggs, N. L.: *Aspects of symmetry in graphs,* Algebraic methods in graph theory Vol. I, II (Szeged, 1978), pp. 27–35, *Colloq. Math. Soc. János Bolyai* **25** North-Holland, Amsterdam-New York, 1981.

[7] Biggs, N. L. and White, A. T.: *Permutation groups and combinatorial structures,* Cambridge Univ. Press, Cambridge, 1979.

[8] Blokhuis, A.: *Characterization of seminuclear sets in a finite projective plane,* J. Geom. **40** (1991), 15–19.

[9] Blokhuis, A., Malnič, A., Marušič, D., Kiss, Gy., Kovács, I., Ruff, J.: *Semiovals contained in the union of three concurrent lines,* J. of Comb. Designes. **15** (2007) 491–501.

[10] Blokhuis, A. and Szőnyi, T.: *Note on the structure of semiovals in finite projective planes,* Discrete Math. **106/107** (1992), 61–65.

[11] Bosma, W., Cannon, J., Playoust, C.: *The* Magma *Algebra System I: The User Language,* J. Symbolic Comput. **24** (1997), 235–265.

[12] Buekenhout, F.: *Characterizations of semi quadrics. A survey,* Colloquio Internazionale sulle Teorie Combinatorie (Roma, 1973), Tomo I, pp. 393–421. Atti dei Convegni Lincei, No. 17, Accad. Naz. Lincei, Rome, 1976.

[13] Cameron, P. J.: *Four lectures on Projective Geometries,* in: Finite Geom. (ed.: Baker, C.A. and Batten, L.M.) Lecture Notes in pure and applied math. **103**, Marcel Dekker (1985), 27–63.

[14] Conway,J. H. Talk given at the Second British Combinatorial Conference at Royal Holloway College, 1971.

[15] Csajbók, B. and Kiss, Gy.: *Notes on semiarcs,* Mediterranean J. Math, submitted

[16] Davydov, A. A.: *Constructions and families of covering codes and saturating sets of points in projective geometry,* IEEE Transactions on Information Theory **41** (1995), 2071–2080.

[17] Davydov, A. A. and Drozhzhina-Labinskaya, A. Yu.: *Constructions, families and tables of binary linear covering codes,* IEEE **40** (1994), 1270–1279.

[18] Davydov, A. A., Faina, G., Marcugini, S. and Pambianco, F.: *Computer search in projective planes for the sizes of complete arcs,* J. Geom. **82** (2005), 50–62.

[19] Dixon, J. D. and Mortimer, B.: *Permutation groups,* Springer-Verlag, New York, 1996.

[20] Dover,J. M.: *Semiovals with large collinear subsets,* J. Geom. **69** (2000), 58–67.

[21] Gardiner, A., Nedela, R., Širáň, J. and Škoviera, M.: *Characterisation of graphs which underlie regular maps on closed surfaces,* J. London Math. Soc. (2) **59** (1999), 100-108

[22] Gács, A.: *On regular semiovals,* J. Algebraic Combin., **23** (2006), 71-77.

[23] Godsil, C. D.: *Algebraic Combinatorics,* Chapman & Hall, New York 1993.

[24] Gordon, D. M.: *The prime power conjecture is true for* $n < 2,000,000$, Electronic J. Combin. 1 R6 (1994).

[25] Gross, J. L., Tucker,T. W.: *Generating all graph coverings by permutation voltage assignment,* Discrete Math. **18** (1977), 273-283.

[26] Hirschfeld, J. W. P. and Storme, L.: *The packing problem in statistics, coding theory and finite projective spaces,* in: Finite Geometries, Development of Mathematics, Kluwer, 2001, 201–246.

[27] Hoffman, A. J. and Singleton,R. R.: *On Moore graphs with diameter* 2 *and* 3*,* IBM J. Res. Develop. **4** (1960), 497–504.

[28] Hubaut, X.: *Limitation du nombre de points d'un* (k, n)*-arc régulier d'un plan projectif fini,* Atti Accad. Naz. Lincei Rend. **8** (1970), 490–493.

[29] Johnson, P. M.: *Semiquadratic sets and embedded polar spaces,* J. Geom. **64** (1999), 102–127.

[30] Kiss, Gy.: *Small semiovals in* $PG(2, q)$*,* J. Geom., **88** (2008), 110-115.

[31] Kiss, Gy., Kovács, I., Kutnar, K., Ruff, J., Šparl, P.: *A note on a geometric construction of large Cayley graphs of given degree and diameter,* Studia Univ. "Babes-Bolyai", Mathematica LIV **3** (2009), 77-84.

[32] Kiss, Gy. and Ruff, J.: *Notes on small semiovals,* Ann. Univ. Sci. Budapest. Eötvös Sect. Math. **47** (2004), 97–105.

[33] Kovács, I., Kutnar, K. and Marušič, D.: *Classification of edge-transitive rose window graphs,* to apper in J. Graph Theory, 2009, 1-16, doi: 10.1002/jgt.20475

[34] Kovács, I., Kutnar, K. and Ruff, J.: *Rose window graphs underlying rotary maps,* Discrete Math. **12** 310 (2010), 1802-1811.

[35] Malnič, A.: *Group actions, coverings and lifts of automorphisms,* Discrete Math. **182** (1998), 203-218.

[36] Malnič, A., Marušič, D. and Potočnik,P.: *Elementary abelian covers of graphs,* J. Algebraic Combin. **20** (2004), 71-97.

[37] Mann, H.B.: *Addition Theorems,* John Wiley, 1965.

[38] Ḿiklavič, S., Potočnik, P. and Wilson, S.: *Consistent cycles in graphs and digraphs,* Graphs and Combin. **23** (2007), 205–216.

[39] Miller, M. and Širaň, J.: *Moore graphs and beyond: A survey of the degree/diameter problem,* Electron. J. Combin., DS14 (2005) 61 pp.

[40] Nagell, T.: *The diophantine equation* $x^2 + 7 = 2^n$, Ark. Mat. **4** (1961), 185–187.

[41] Potočnik, P. and Wilson, S.: *A Census of edge-transitive tetravalent graphs,*
`http://jan.ucc.nau.edu/~swilson/C4Site/index.html`

[42] Rédei, L.: *Die neue Theorie der endlichen abelschen Gruppen und Verallgemeinerung des Hauptsatzes von Hajós,* Acta Math. Acad. Sci. Hungar. **16** (1965), 329–373.

[43] Suetake, C.: *Two families of blocking semiovals,* European J. Combin. **21** (2000), 973–980.

[44] Szabó, S.: *Topics in Factorizations of Abelian Groups,* Birkhäuser Verlag, Basel-Boston-Berlin 2004.

[45] Szőnyi, T.: *Combinatorial problems for abelian groups arising from geometry,* Period. Polytech. Transportation Engrg. **19** (1991), no. 1-2, 91–100.

[46] Thas, J. A.: *On semiovals and semiovoids,* Geom. Dedicata 3 (1974), 229–231.

[47] Wilson, S.: *Rose Window Graphs,* Ars Math. Contemp. **1** (2008), 7–19.
`http://amc.imfm.si/index.php/amc/issue/view/5`

[48] Wilson, S.: *Operators over regular maps,* Pacific J. Math. **81** (1979), 559-568.

[49] *The (Degree,Diameter) Problem for Graphs,* A World Combinatorics Exhange resource at
`http://www-mat.upc.es/grup\_de\_grafs/oldpage.html`.