Eötvös Loránd University

Institute of Mathematics

Ph.D. thesis

Some graph theoretic aspects of finite geometries

Tamás Héger

Doctoral School: Mathematics

Director: Miklós Laczkovich, D.Sc.

Professor, Member of the Hungarian Academy of Sciences

Doctoral Program: Pure Mathematics

Director: András Szűcs, D.Sc.

Professor, Corresp. Member of the Hungarian Academy of Sciences

Supervisors:

András Gács, Ph.D.

Tamás Szőnyi, D.Sc.

Professor

Department of Computer Science

Faculty of Science, Eötvös Loránd University

Budapest, 2013

Contents

Introduction

The results presented in this thesis are from the fields of finite geometry and graph theory, mainly from their intersection. The emphasis is on the finite geometrical viewpoint, though most of the research was motivated by graph theoretical questions. Two of the examined areas, the problem of cages and the Zarankiewicz-problem, have extremal combinatorial origins, and have attracted a considerable amount of interest since the middle of the last century. It is well-known that generalized polygons play a prominent role in some particular cases of the cage-problem, just as designs do in the Zarankiewicz-problem. The idea we consider in this work regarding these problems is that the known extremal structures may contain substructures that provide us other valuable constructions. This resembles the general phenomenon of combinatorial stability: in many cases, almost extremal structures can be obtained from extremal ones by subtle modifications. We mainly investigate projective planes, which can be considered as generalized triangles and as symmetric 2-designs as well, but the more general cases will also be touched.

We also consider two general notions from graph theory that become particularly interesting in the setting of finite projective planes. The concept of semi-resolving sets is motivated by localizational questions in graphs, and their study in this setting was proposed by R. F. Bailey. In the theory of hypergraph coloring, the upper chromatic number is the counterpart of the classical chromatic number in some sense, and its study has been intensively encouraged by V. Voloshin. Projective planes, considered as hypergraphs, are naturally arising examples to investigate this problem for, and their study was started in the mid-nineties.

While preparing this thesis, I realized that domination supplies another common graph theoretical background for many of the problems discussed here. Therefore I decided to introduce and use this notion, mainly in the study of (k, g)-graphs.

Besides their graph theoretical motivations, the problems in this work are joined by their finite geometrical aspects as well. The substructures of projective planes we need to study regarding the problem of cages are in connection with weighted multiple blocking sets, while semi-resolving sets and colorings that reach the upper chromatic number both turn out to be closely related to double blocking sets. As for the techniques, the polynomial method plays a crucial role by supplying important information about the structures in question, which information can be used in further combinatorial arguments.

Let us outline the main points of the thesis. In Chapter 1 we review the main definitions and results that we need in the sequel. As three out of the four problems are related to multiple blocking sets, we collect and treat our results regarding these separately in Chapter 2. There we show a unique reducibility result for t-fold blocking sets in $\mathrm{PG}(2,q)$, and give a construction for a small double blocking set in $\mathrm{PG}(2,p^h)$, p an odd prime, $h \geq 3$ odd. The latter result was motivated by the tight connection with the upper chromatic number of $\mathrm{PG}(2,q)$. The next four chapters are devoted to the above mentioned problems. In Chapter 3 we study perfect t-dominating sets in generalized n-gons to construct small $(k,2n)$-graphs, and give a characterization result in $\mathrm{PG}(2,q)$. The main result of Chapter 4 is that a small semi-resolving set for $\mathrm{PG}(2,q)$ can be extended to a double blocking set by adding at most two points to it. As a corollary, we obtain a lower bound on the size of a blocking semioval in $\mathrm{PG}(2,q)$. In Chapter 5 we establish an exact result on the upper chromatic number of $\mathrm{PG}(2,q)$ in terms of the size of the smallest double blocking set. Finally, in Chapter 6, we discuss Zarankiewicz's problem and give several exact values of Zarankiewicz numbers. Our guide in the ordering of these chapters was the role of polynomial techniques used in them. Let us underline that the key tool in Chapters 3 and 4 is a lemma newly developed by Tamás Szőnyi and Zsuzsa Weiner. For the sake of completeness, we give the proof of this lemma in the Appendix.

In general, we use the words Theorem, Proposition, Lemma etc. when referring to our original results, while the word Result is used to denote the fruits of other authors' work. The vast majority of the thesis is based on the six articles denoted by capital letters in the bibliography, which all have been published or accepted for publication in peer-reviewed journals.

Chapter 1

Preliminary definitions and results

1.1 Finite fields and polynomials

We denote by $\mathrm{GF}(q)$ the finite field (Galois field) of order q and $\mathrm{GF}(q)^* = \mathrm{GF}(q) \setminus \{0\}$ is the multiplicative group of $\mathrm{GF}(q)$. For any field $\mathbb{F}$, $\mathbb{F}[X_1, \ldots, X_n]$ denotes the polynomial ring in n variables over $\mathbb{F}$. For $f, g \in \mathbb{F}[X_1, \ldots, X_n]$, $\gcd(f, g)$ denotes the greatest common divisor of f and g, and $\deg(f)$ is the total degree of f. If we want to emphasize the variables taken into account in the degree of the polynomial, we list them as a subscript of deg. In case of a geometric setting, we use upper case letters to denote variables, and use the same letter in lower case when substituting an element of $\mathbb{F}$ into the respective variable. Recall that for any element $x \in \mathrm{GF}(q)^*$, we have $x^{q-1} = 1$; $x^q = x$ for all $x \in \mathrm{GF}(q)$; and $x \mapsto x^p$ is an automorphism of $\mathrm{GF}(q)$, where p is the characteristic of the field.

Definition 1.1.1. *Let $0 \not\equiv f \in \mathbb{F}[X_1, \ldots, X_n]$ for a field $\mathbb{F}$, and suppose that $\boldsymbol{a} \in \mathbb{F}^n$ is a zero of f. The* multiplicity of the zero $\mathbf{a}$ *is defined as the lowest degree that occurs in $f(X_1 + a_1, \ldots, X_n + a_n)$ (which is a positive number). By convention, every element of $\mathbb{F}^n$ is a zero of the zero polynomial of multiplicity t for every positive integer t.*

We say that a polynomial is fully reducible over the field $\mathbb{F}$ if it is the product of some linear factors over $\mathbb{F}$. If a polynomial of $\mathbb{F}[X]$ is fully reducible, then the number of its roots (counted with multiplicities) is equal to its degree. Note that every element of $\mathrm{GF}(q)$ is a root of $X^q - X \in \mathrm{GF}(q)[X]$ with multiplicity one, hence $X^q - X = \prod_{a \in \mathrm{GF}(q)} (X - a)$ is fully reducible.

We will use the following multiplicity version of Alon's combinatorial Nullstellensatz.

RESULT 1.1.2 (Ball–Serra [16]). *Let $\mathbb{F}$ be any field, $f \in \mathbb{F}[X_1, \ldots, X_n]$, and let $S_1, \ldots, S_n$ be finite non-empty subsets of $\mathbb{F}$. For all $1 \leq i \leq n$, define*

$$g_i(X_i) = \prod_{s \in S_i} (X_i - s).$$

Let $\mathbb{N}_t^n = \{(a_1, \ldots, a_n) \in \mathbb{Z}^n \colon a_1 + \ldots + a_n = t, a_1 \geq 0, \ldots, a_n \geq 0\}$. If f has a zero of multiplicity at least t at every point of $S_1 \times \ldots \times S_n$, then there exist polynomials $h_{\underline{\boldsymbol{a}}} \in \mathbb{F}[X_1, \ldots, X_n]$, $\underline{\boldsymbol{a}} \in \mathbb{N}_t^n$, for which $\deg(h_{\underline{\boldsymbol{a}}}) \leq \deg(f) - \sum_{i=1}^n a_i |S_i|$ and

$$f = \sum_{\underline{\boldsymbol{a}} \in \mathbb{N}_t^n} g_1^{a_1} \cdot \ldots \cdot g_n^{a_n} h_{\underline{\boldsymbol{a}}}.$$

The following, recent theorem will be a crucial tool as well. For $z \in \mathbb{Z}$, let $z^+ := \max\{0, z\}$.

RESULT 1.1.3 (Szőnyi–Weiner Lemma [71, 69]). *Let $u, v \in \mathbb{F}[X, Y]$. Suppose that the term $X^{\deg(u)}$ has non-zero coefficient in $u(X, Y)$ (that is, $\deg(u(X, Y)) = \deg(u(X, y))$ for every element $y \in \mathbb{F}$). Let $k_y := \deg \gcd(u(X, y), v(X, y))$ for any $y \in \mathbb{F}$. Then for an arbitrary $y \in \mathbb{F}$,*

$$\sum_{y' \in \mathbb{F}} (k_{y'} - k_y)^+ \leq (\deg u(X, Y) - k_y)(\deg v(X, Y) - k_y).$$

We give the proof of this lemma in the Appendix.

1.2 Graphs

We only consider finite, simple, undirected graphs. $G = (V; E)$ denotes a graph with vertex-set V and edge-set E, and $G = (A, B; E)$ denotes a bipartite graph with vertex classes A and B, and edge-set E. Two vertices are called adjacent or neighbors if there is an edge connecting them. The set of neighbors of v is denoted by $N(v)$. The number of neighbors of a vertex v is called the degree of v, and we denote it by $d(v)$. A graph is k-regular if every vertex has exactly k neighbors. The length of a path or a cycle is the number of edges contained in it. C_n stands for a cycle of length n. The girth of a graph G, in notation $g(G)$, is the length of the shortest cycle in it.

Let x and y be two vertices. The distance of x and y, denoted by $d(x, y)$, is the length of the shortest path between x and y. Should there be no such path, let $d(x, y) = \infty$. For two vertex-sets $X \subset V$ and $Y \subset V$, let $d(X, Y) = \min\{d(x, y) \colon x \in X, y \in Y\}$. If X or Y has one element only, we write for example $d(x, Y)$ instead of $d(\{x\}, Y)$. A ball of center $v \in V$ and radius $r \in \mathbb{N}$ is $B^r(v) = \{u \in V : d(v, u) \leq r\}$.

The adjacency matrix of G is the matrix $A = A(G)$ of $\{0, 1\}^{V \times V}$, where $A_{u,v} = 1$ if and only if u and v are adjacent $(u, v \in V)$.

In the following we introduce the general graph theoretical notion called domination. We mostly follow the book by Haynes, Hedetniemi and Slater [45]. In the upcoming definitions we suppose that a graph $G = (V; E)$ is given.

DEFINITION 1.2.1. *We say that a vertex v* dominates *the vertex u if either $u = v$ or u is adjacent to v. Accordingly, a set S of vertices dominates the set $S \cup \bigcup_{v \in S} N(v)$.*

DEFINITION 1.2.2. *A vertex-set $S \subsetneq V$ is called a* t-fold dominating set, *if for all $v \in V \setminus S$ we have $|N(v) \cap S| \geq t$; that is, every vertex is an element of S or has at least t neighbors in S. In other words, every vertex $v \notin S$ is dominated by S at least t times.*

As usual, we may omit the prefix "1-fold", and we may also substitute the word "double" for the prefix "2-fold".

DEFINITION 1.2.3. *A t-fold dominating set S is called* perfect *(abbreviated as t-PDS), if for all $v \in V \setminus S$ we have $|N(v) \cap S| = t$; that is, every vertex outside S has precisely t neighbors in S.*

There is a frequently investigated variation of domination, called total domination, where self-domination is not allowed.

DEFINITION 1.2.4. *A vertex-set $S \subsetneq V$ is called a* t-fold total dominating set, *if for all $v \in V$ we have $|N(v) \cap S| \geq t$; that is, every vertex has at least t neighbors in S (even the elements of S). In other words, every vertex v is dominated at least t times by $S \setminus \{v\}$.*

PROPOSITION 1.2.5. *In a bipartite graph $G = (A, B; E)$, a proper vertex-set S is a t-fold total dominating set iff $S \cap A$ dominates B at least t times and $S \cap B$ dominates A at least t times.*

Proof. As any vertex dominates vertices only from the other class, the assertion is trivial. □

Thus in bipartite graphs a total dominating set may be also called a split dominating set, while an ordinary dominating set may be called a non-split dominating set.

DEFINITION 1.2.6. *Let $G = (A, B; E)$ be a bipartite graph. A vertex-set S is a* t-fold semi-dominating set*, if S is a subset of one of the vertex classes, and it dominates the other class at least t times.*

In case of bipartite graphs, discussing semi-dominating sets is also interesting. In fact, in finite geometry a huge amount of research has been done on t-fold semi-dominating sets (and thus, though accidentally, on total dominating sets). In the incidence graph of a finite projective or affine plane a t-fold semi-dominating set is called either a t-fold blocking set or a t-fold covering set, depending on whether it dominates the lines or the points, respectively. We will discuss these structures later.

Non-split dominating sets have not been in the center of finite geometrical research. When looking for certain (k, g)-graphs in Chapter 3, we will make use of t-fold perfect dominating sets in the incidence graph of projective planes and other generalized polygons.

Domination in graphs has several variations. For example, a dominating set S is called locating if $N(v) \cap S$ is unique for each vertex $v \notin S$. Other localizational questions lead to the definition of a resolving set for a graph. We say that a vertex-set $S = \{s_1, \ldots, s_k\}$ resolves the vertex v if the distance list $(d(s_1, v), \ldots, d(s_k, v))$ is unique (so we can identify v by its distance list with respect to S). The set S is called a resolving set if it resolves all vertices of the graph. As in case of dominating sets, we may define semi-resolving sets for bipartite graphs. Chapter 4 is devoted to semi-resolving sets for the incidence graphs of projective planes.

1.3 Incidence structures

An incidence structure is a triplet $\Psi = (A, B; \mathcal{I})$ where A and B are disjoint, nonempty sets and $\mathcal{I} \subset A \times B$ is a relation between the elements of A and B called incidence. Throughout this work we consider finite incidence structures, that is, A and B are finite sets. The elements of $A \cup B$ and $\mathcal{I}$ will be called objects and flags, respectively; a non-incident pair of elements is called an anti-flag. Usually the set A is considered as a point-set, while the elements of B are regarded as lines or blocks, depending on the context. If $(a, b) \in \mathcal{I}$ for some $a \in A$, $b \in B$, we say that a is incident with b, or b is incident with a, or a and b are incident.

The dual of Ψ is $\Psi^T = (B, A; I^T)$, where $(b, a) \in \mathcal{I}^T \iff (a, b) \in \mathcal{I}$ for all $a \in A$ and $b \in B$. An incidence structure $\Psi = (A, B; \mathcal{I})$ is isomorphic to another one $\Psi' = (A', B'; \mathcal{I}')$ iff there is a bijective mapping $\varphi\colon A \cup B \to A' \cup B'$ such that $\varphi(A) = A'$, $\varphi(B) = B'$, and $(a, b) \in \mathcal{I} \iff (\varphi(a), \varphi(b)) \in \mathcal{I}'$. An incidence structure Ψ is called self-dual if it is isomorphic to Ψ^T.

Various sets of axioms may be used to restrict our attention to a specific class of incidence structures. We may call a class self-dual if its axioms are symmetric in A and B (that is, an incidence structure Ψ satisfies the axioms iff Ψ^T does). For such classes, the principle of duality can be applied: if for an incidence structure Ψ we can deduce a statement from the axioms, then we also have the dual statement in Ψ (that is, we may interchange the role of the sets A and B in the statement), as the same arguments work in Ψ^T. In case of self-dual class (which means generalized polygons in the context of this work), one can distinguish A and B only artificially. However, it is worth noting that an incidence structure of a self-dual class may not be self-dual.

Sometimes blocks (or lines) are identified with the set of points they are incident with, which allows us to consider an incidence structure as a set system or a hypergraph. This justifies the notation $a \in b$ to express $(a, b) \in \mathcal{I}$. Thus many times we just write $\Psi = (A, B)$ for an incidence structure without indicating the incidence relation, which we think of as the $\in$ relation. However, in case of a self-dual class or structure, this otherwise comfortable approach regrettably breaks the symmetry between the sets A and B, which is considerably unfortunate. Therefore, in a self-dual context, to conciliate our natural demands for comfort and symmetry, we will simultaneously treat an object of an incidence structure as a standalone being and as the set of objects incident with it as well. This allows us to write $a \in b$ or $b \in a$ to indicate that a and b are incident. Moreover, as it is common in the case of a geometric setting, we may denote the common point of two lines e and ℓ by $e \cap \ell$, for example; furthermore, we might also denote the line joining the points P and Q by $P \cap Q$ (besides the standard notation PQ or $\overline{PQ}$). If, for some $x \in A \cup B$, we want to emphasize that we consider the set of objects x is incident with, we will use the notation $[x]$ defined as $[x] = \{y \in A \cup B \colon x \in y\}$. Then, naturally, the notation $y \in [x]$ and $x \in [y]$ are also completely satisfactory to express x and y being incident; and, indeed, $[P] \cap [Q]$ is the line connecting P and Q.

The triplet $(A, B; \mathcal{I})$ can be regarded as a bipartite graph with vertex classes A and B and edge-set $\mathcal{I}$ (more precisely, the edge-set should be $\{\{a, b\} \colon (a, b) \in \mathcal{I}\}$). The bipartite graph arising from the incidence structure Ψ is called the incidence graph or Levi-graph of Ψ, and will be denoted by $G(\Psi)$. Two graphs are isomorphic iff there is a bijection between their vertex-sets that maps edges to edges and non-edges to non-edges. If two incidence structures Ψ and Ψ' are isomorphic, then $G(\Psi)$ and $G(\Psi')$ are also isomorphic. Moreover, as graph isomorphism may interchange the vertex classes, $G(\Psi) \cong G(\Psi'^T)$ follows as well. As there exist incidence structures that are not self-dual, $G(\Psi) \cong G(\Psi')$ does not imply $\Psi \cong \Psi'$.

Usually we will not distinguish an incidence structure from its incidence graph; hence we will unscrupulously mix the graph theoretical terminology and notation with the geometrical ones. In this manner, we may talk about a subgraph of a projective plane when thinking of a subgraph of the incidence graph of the projective plane, for example.

Ψ can also be represented by a 0–1 matrix $M(\Psi)$ called the *incidence matrix* of Ψ, defined as follows. Let $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_m\}$ be any ordering of A and B, respectively, where $|A| = n$ and $|B| = m$. Then $M(\Psi) \in \{0,1\}^{n\times m}$, and $M_{i,j} = 1$ iff a_i and b_j are incident in Ψ. Ψ and Ψ' (considered as incidence structures) are isomorphic iff there exist permutation matrices $P \in \{0,1\}^{n\times n}$ and $Q \in \{0,1\}^{m\times m}$ such that $PM(\Psi)Q = M(\Psi')$. Note that under a suitable ordering of its vertices, the adjacency matrix of $G(\Psi)$ is the block-matrix

$$\begin{pmatrix} M(\Psi) & \mathbf{0} \\ \mathbf{0} & M(\Psi)^T \end{pmatrix}.$$

1.4 Generalized polygons

In the geometric context of generalized polygons, we consider the two sets of an incidence structure as points and lines, and so denote them by $\mathcal{P}$ and $\mathcal{L}$, respectively. We say that some points (lines) are collinear (concurrent), if there exists a line (point) incident with all of them; and a set of points (lines) is said to be in general position if no three of them are collinear (concurrent).

DEFINITION 1.4.1 (Generalized polygon, GP). *Let $n \geq 3$, $s,t \geq 1$ be integers. An incidence structure is a* generalized n-gon of order (s,t) *if and only if the following hold:*

GP1: every point is incident with $s+1$ lines;

GP2: every line is incident with $t+1$ points;

GP3: the diameter and the girth of its incidence graph is n and $2n$, respectively.

From GP3 it follows that if $d(x, y) \leq n-1$, then there is a unique path of length $\leq n-1$ connecting x to y. Note that the axioms of generalized polygons are symmetric in points and lines, that is, the dual of a GP of order (s,t) is a GP of order (t,s). The deep result of Feit and Higman [37] claims that generalized n-gons of order (q,q), $q \geq 2$, exist only if $n = 3$, 4 or 6; these are called a generalized triangle (or a projective plane), a generalized quadrangle (GQ), and a generalized hexagon (GH) of order q, respectively. Generalized polygons of order q are known to exist if q is a power of a prime, but no example has been found otherwise so far. It is easy to compute that a generalized n-gon of order (q,q) has $\sum_{i=0}^{n-1} q^i$ points and the same number of lines.

We also mention that one may give alternative definitions for a GP. For example, a projective plane is commonly defined as follows.

DEFINITION 1.4.2. *An incidence structure* $(\mathcal{P}, \mathcal{L})$ *is a* projective plane *if and only if it satisfies the following axioms:*

1. *any two points have a unique line incident with both;*
2. *any two lines have a unique point incident with both;*
3. *there exist four points in general position.*

From these properties it follows that there exists a number $q \geq 2$ such that our incidence structure is a generalized triangle of order (q,q). The notation Π_q always refers to a projective plane of order q.

DEFINITION 1.4.3. *An incidence structure* $(\mathcal{P}, \mathcal{L})$ *is a* degenerate projective plane *if it satisfies the first two axioms of a projective plane (Definition 1.4.2) but not the third. If the maximal number of points in general position in a degenerate projective plane is at most two, then it is of* type π_1*; if this number is three, then it is of* type π_2.

In a degenerate projective plane of type π_1 there is an incident point-line pair (P, ℓ) such that all points are incident with ℓ and all lines are incident with P; in a degenerate projective plane of type π_2 there is a non-incident point-line pair (P, ℓ) such that every point except P is incident with ℓ, and every line except ℓ is incident with P. Degenerate projective planes are not generalized triangles except for the ordinary triangle.

In case of generalized quadrangles, GP3 is commonly replaced by GQ3: for all $P \in \mathcal{P}$ and $\ell \in \mathcal{L}$ such that $P \notin \ell$, there exists a unique line $e \in \mathcal{L}$ such that $P \in e$ and e intersects ℓ. We end this section by giving some further definitions.

DEFINITION 1.4.4. *Let* $(\mathcal{P}, \mathcal{L})$ *be a GP,* $\mathcal{S} \subset \mathcal{P}$, $\ell \in \mathcal{L}$. *Then* ℓ *is a* t-secant *to* S *iff* $|\ell \cap S| = t$. *A* 0*-secant or a* 1*-secant is also called a skew or tangent (line) to* S. *A* $(> t)$*-secant to* S *is a line intersecting* S *in more than* t *points;* $(\geq t)$, $(< t)$, *and* $(\leq t)$*-secants are defined analogously.*

DEFINITION 1.4.5. *Let* $(\mathcal{P}, \mathcal{L})$ *be a GP,* $\mathcal{S} \subset \mathcal{P}$, $\mathcal{R} \subset \mathcal{L}$. *We say that* $\mathcal{S}$ blocks *the line* ℓ *if* $\ell \cap \mathcal{S}$ *is nonempty; dually,* $\mathcal{R}$ covers *a point* P *if* $P \cap \mathcal{R}$ *is nonempty.*

1.5 Projective and affine spaces

First let us give the combinatorial definition of an affine plane.

DEFINITION 1.5.1. *An incidence structure* $(\mathcal{P}, \mathcal{L})$ *is an* affine plane *if and only if the following hold:*

1. *any two points have a unique line incident with both;*
2. *for any line* ℓ *and any point* $P \notin \ell$ *there exists a unique line* e *such that* $P \in e$ *and* $e \cap \ell$ *is empty;*
3. *there exist three points in general position.*

If two lines of an affine plane do not intersect each other, we call them parallel. One can construct an affine plane from a projective plane by removing from it a line together with its points. It is well-known that any affine plane has q^2 points and $q^2 + q$ lines for some integer $q \geq 2$, which is called the order of the affine plane; moreover, every affine plane of order q can be embedded into a unique projective plane of order q. This follows from the simple fact that parallelism is an equivalence relation for the lines of the affine plane.

In the sequel we define n-dimensional projective and affine spaces over the field $\mathrm{GF}(q)$, though, in fact, we will only consider them for $n = 3$. The n dimensional projective space over the finite field $\mathrm{GF}(q)$, denoted by $\mathrm{PG}(n, q)$, can be defined as follows. Take the linear space $V = \mathrm{GF}(q)^{n+1}$. The point-set $\mathcal{P}$ of $\mathrm{PG}(n, q)$ is the set of one dimensional subspaces of V; and in general, the set $\mathcal{F}_k$ of flats of rank k of $\mathrm{PG}(n, q)$, $0 \leq k \leq n$, is the set of $k + 1$ dimensional subspaces of V. Note that $\mathcal{F}_0 = \mathcal{P}$, $\mathcal{F}_n = \{V\}$. The flats are ordered by inclusion. Flats of rank 0, 1, 2, 3 and $n - 1$ are also called a point, a line, a plane, a solid and a hyperplane of $\mathrm{PG}(n, q)$, respectively. The set $\mathcal{F}_1$ of lines is also denoted by $\mathcal{L}$. We write $F \in \mathrm{PG}(n, q)$ to denote that F is a flat of $\mathrm{PG}(n, q)$.

Points of $\mathrm{PG}(n,q)$ can be represented by any non-zero vector v spanning the respective one dimensional subspace of V. Two vectors v and w represent the same point of $\mathrm{PG}(n,q)$ if and only if $w=\lambda v$ for some $\lambda \in \mathrm{GF}(q)^*$; hence the coordinates of the representatives are well-defined up to a non-zero scalar multiplier. Such $(n+1)$-tuples are called homogeneous coordinates; in notation, we write $(v_1 : v_2 : \ldots : v_{n+1})$. A hyperplane has a one dimensional orthogonal complement in V, so it can also be represented by a homogeneous $(n+1)$-tuple. To distinguish the representatives of points and hyperplanes, we will use the notation $[v_1 : v_2 : \ldots : v_{n+1}]$ for the latter. Note that a point (v) is in the hyperplane $[w]$ if and only if their inner product, vw (more precisely, vw^T if the vectors are considered as rows), is zero.

The n-dimensional affine plane over $\mathrm{GF}(q)$, denoted as $\mathrm{AG}(n,q)$, can be derived from $\mathrm{PG}(n,q)$ in the following way: let $H_\infty = \{(v) \in \mathrm{PG}(n,q) : v_{n+1} = 0\} = [0 : \ldots : 0 : 1]$, and let the point-set $\mathcal{P}^A$ of $\mathrm{AG}(n,q)$ be $\mathcal{P} \setminus H_\infty$. The set $\mathcal{F}_k^A$ of k dimensional flats of $\mathrm{AG}(n,q)$ is $\{\mathcal{P}^A \cap F \colon F \in \mathcal{F}_k, F \not\subset H_\infty\}$, $k=1,\ldots,n$. By the homogeneity of the coordinates, we may choose $(v) \in \mathrm{AG}(n,q)$ so that $v_{n+1}=1$, and identify the points of $\mathrm{AG}(n,q)$ with the points of $\mathrm{GF}(q)^n$ by the mapping $(v_1 : \ldots : v_n : 1) \mapsto (v_1, \ldots, v_n)$. Usually we consider $\mathrm{AG}(n,q)$ as embedded into $\mathrm{PG}(n,q)$. In this case, H_∞ is called the hyperplane at infinity, a point $(v_1 : \ldots : v_n : 1) = (v_1, \ldots, v_n)$ is called an affine point, while the points of H_∞ are called ideal points or directions.

In case of $n=2$, that is, the affine plane $\mathrm{AG}(2,q)$ embedded into $\mathrm{PG}(2,q)$, $H_\infty = \ell_\infty$ is called the line at infinity; by homogeneity, its points can be represented in the form $(1 : m : 0)$, $m \in \mathrm{GF}(q)$ or $(0 : 1 : 0)$. We will also denote these points by (m) $(m \in \mathrm{GF}(q))$ and (∞), respectively. Also, we may identify a set $D \subset \mathrm{GF}(q)$ with the set of directions $\{(m) \colon m \in D\}$. A line of $\mathrm{PG}(2,q)$ different from ℓ_∞ is called an affine line. An affine line $[m : -1 : b]$ is incident with the points $\{(x : y : 1) = (x,y) \colon y = mx + b\} \cup \{(1 : m : 0)\}$, and m is called the slope of the line. A line with representative of form $[-1 : 0 : c]$ is incident with the points $\{(x : y : 1) = (x,y) \colon x = c\} \cup \{(0 : 1 : 0)\}$; such lines are called vertical. If two affine lines intersect at the line at infinity, we call them parallel. The set of q pairwise parallel lines incident with the same point of the line at infinity is called a parallel class.

In a projective plane $\Pi_q = (\mathcal{P}, \mathcal{L})$, we may count the cardinality of a point-set $S \subset \mathcal{P}$ with respect to a point P. If $P \notin S$, then $|S| = \sum_{\ell \ni P} |\ell \cap S|$; if $P \in S$, then $|S| = 1 + \sum_{\ell \ni P}(|\ell \cap S| - 1)$. To indicate that we are considering the intersections of all the lines through a given point P and a point-set, we might say that we look around from P.

The projective plane $\mathrm{PG}(2,q)$ is well-known to have a large automorphism group. In particular, any ordered quadruple of points in general position can be mapped into any other such quadruple by an automorphism of the plane. Thus we may choose the coordinate system quite freely, e.g., we may take any line ℓ to be the line at infinity and any two points of ℓ to be (∞) and (0) when considering $\mathrm{AG}(2,q)$ embedded into $\mathrm{PG}(2,q)$.

Note that $\mathrm{PG}(2,q)$ is self-dual: the mapping from $\mathrm{PG}(2,q)$ to $\mathrm{PG}(2,q)^T$ defined by $(x:y:z) \mapsto [x:y:z]$ and $[a:b:c] \mapsto (a:b:c)$ clearly preserves incidence. For more information and related topics we refer to the book [46].

1.5.1 The standard equations

Next we give a well-known, simple but often useful counting argument that may be referred to as the standard equations. Let $\mathcal{B} \subset \mathcal{P}$ be a point-set in an arbitrary projective plane $\Pi_q = (\mathcal{P}, \mathcal{L})$ of order q. Let n_i denote the number of i-secant lines to $\mathcal{B}$. Then we have

$$\sum_{i=0}^{q+1} n_i = |\mathcal{L}| = q^2+q+1,$$

$$\sum_{i=0}^{q+1} i n_i = |\{(P,\ell)\colon P \in \mathcal{B}, \ell \in \mathcal{L}, P \in \ell\}| = |\mathcal{B}|(q+1),$$

$$\sum_{i=0}^{q+1} i(i-1) n_i = |\{(P,Q,\ell)\colon P,Q \in \mathcal{B};\ P \neq Q;\ \ell \in \mathcal{L};\ P,Q \in \ell\}| = |\mathcal{B}|(|\mathcal{B}|-1).$$

1.5.2 Special substructures of projective planes

Here we collect some substructures of projective planes and some of their properties that will be needed in the sequel.

Subplanes

We call a pair $\Pi' = (\mathcal{P}_0, \mathcal{L}_0)$ of a point-set and a line-set of a projective plane Π_q of order q a closed system, if the intersection point of any two lines of $\mathcal{L}_0$ is in $\mathcal{P}_0$, and dually, the line joining any two points of $\mathcal{P}_0$ is in $\mathcal{L}_0$. If there are four points in general position in $\mathcal{P}_0$, then Π' is a projective plane on its own right; in this case Π' is called a subplane of Π. Note that any line intersects a subplane of order s in 0, 1 or $s+1$ points. It is easy to derive the following observation attributed to R. H. Bruck.

RESULT 1.5.2 (Bruck [26]). *Suppose that a projective plane of order q has a proper subplane of order s. Then either $s = \sqrt{q}$ or $s^2 + s \leq q$.*

If a closed system Π' does not contain four points in general position, then it is a degenerate projective plane, and so it is called a degenerate subplane of type π_1 or π_2 (cf. Definition 1.4.3). The number of points and lines of a degenerate subplane of type π_1 in Π_q may be different, but each number is at most $q+1$. A degenerate subplane of type π_2 in Π_q has equally many points and lines, at most $q+2$ of each. It is well-known that all non-degenerate subplanes of $\mathrm{PG}(2, p^h)$, p a prime, have order p^k, where k divides h. Thus $\mathrm{PG}(2, p)$, p prime, does not have non-degenerate subplanes.

A subplane of order $\sqrt{q}$ is called a Baer subplane, and it intersects every line in either 1 or $\sqrt{q}+1$ points. It is known that in any projective plane Π_q, the intersection of two Baer subplanes is a closed system with equally many points and lines [24, 68]. In $\mathrm{PG}(2, q)$, four points in general position determine a unique Baer subplane; thus the intersection of two distinct Baer subplanes is either empty or it is a degenerate subplane of both Baer subplanes, and so it has at most $\sqrt{q}+2$ points.

Multiple blocking sets

DEFINITION 1.5.3. *A point-set $\mathcal{B}$ in $\Pi_q = (\mathcal{P}, \mathcal{L})$ is a t-*fold blocking set *if $|\ell \cap \mathcal{B}| \geq t$ for all $\ell \in \mathcal{L}$. One-fold and two-fold blocking sets are also called a* blocking set *and a* double blocking set, *respectively. A line-set $\mathcal{S}$ in $\Pi_q = (\mathcal{P}, \mathcal{L})$ is a t-*fold covering set *if $|P \cap \mathcal{S}| \geq t$ for all $P \in \mathcal{P}$. Note that this is the dual of a t-fold blocking set.*

We remark that a blocking set is also commonly defined as a point-set which intersects every line, but does not contain a line. In the language of hypergraphs, t-fold blocking sets are called t-transversals.

DEFINITION 1.5.4. *Let $\mathcal{B}$ be a t-fold blocking set in $\Pi_q = (\mathcal{P}, \mathcal{L})$. A point $P \in \mathcal{B}$ is* essential, *if $\mathcal{B} \setminus \{P\}$ is not a t-fold blocking set; equivalently, if there is a t-secant to $\mathcal{B}$ through P. $\mathcal{B}$ is* minimal, *if all its points are essential; equivalently, if it does not contain a smaller t-fold blocking set.*

DEFINITION 1.5.5. *The size of the smallest t-fold blocking set in Π_q is denoted by $\tau_t(\Pi_q)$, and it is called the* t-blocking number *of Π_q. We write simply τ_t if the context makes clear which projective plane the notation regards to.*

Blocking sets and multiple blocking sets are widely studied objects. We will use many results regarding these. Note that by duality, we have the same results for (multiple) covering sets.

A point-set containing a line is always a blocking set. A Baer subplane is well-known to be a blocking set. The union of the point-set of any t pairwise disjoint Baer subplanes is a t-fold blocking set. Such a t-fold blocking set intersects every line in t or $\sqrt{q}+t$ points. If q is a square, then $\mathrm{PG}(2,q) = (\mathcal{P},\mathcal{L})$ can be partitioned into pairwise disjoint Baer subplanes $(\mathcal{P}_i,\mathcal{L}_i)$, $1 \le i \le q-\sqrt{q}+1$, so that $\mathcal{P} = \cup_{i=1}^{q-\sqrt{q}+1}\mathcal{P}_i$ and $\mathcal{L} = \cup_{i=1}^{q-\sqrt{q}+1}\mathcal{L}_i$.

The next theorem is also referred to as the Bruen–Pelikán theorem.

RESULT 1.5.6 (Bruen [27]). *A blocking set $\mathcal{B}$ in Π_q not containing a line has at least $q+\sqrt{q}+1$ points. In case of equality $\mathcal{B}$ is a Baer subplane.*

RESULT 1.5.7 (Ball–Blokhuis [13]). *Let $q \ge 9$ be a square prime power. Then $\tau_2(\mathrm{PG}(2,q)) = 2(q+\sqrt{q}+1)$.*

RESULT 1.5.8 (Blokhuis–Storme–Szőnyi [23]). *Let $\mathcal{B}$ be a t-fold blocking set in $\mathrm{PG}(2,q)$ of size $t(q+1)+C$. Let $c_2 = c_3 = 2^{-1/3}$ and $c_p = 1$ for $p > 3$. Then*

1. *if $q = p^{2d+1}$ and $t < q/2 - c_pq^{2/3}/2$, then $C \ge c_pq^{2/3}$;*
2. *if q is a square, $t < \min\{q^{1/4}/2, c_pq^{1/6}\}$, and $C < c_pq^{2/3}$, then $\mathcal{B}$ contains the union of t disjoint Baer subplanes. Consequently, under the same conditions, $\tau_t(\mathrm{PG}(2,q)) = t(q+\sqrt{q}+1)$.*

REMARK 1.5.9. *In particular, if $\mathcal{B}$ is a double blocking set in $\mathrm{PG}(2,q)$, q a square, $q > 256$, and $|\mathcal{B}| \le 2q+2\sqrt{q}+11 = \tau_2+9$, then $\mathcal{B}$ contains two disjoint Baer subplanes.*

Proof. We only verify the respective assumptions of Result 1.5.8. First, $2 = 256^{1/4}/2 < q^{1/4}/2$. Second, we need $9 < c_pq^{2/3} - 2\sqrt{q}$. As $q > 256$ and q is a square, we have $q \ge 17^2 = 289$. In the case of $c_p = 1$, we obtain $9.71 < 289^{2/3} - 34 \le q^{2/3} - 2\sqrt{q}$. In the case of $c_p = 2^{-1/3}$, that is, $p \in \{2,3\}$, we have $q \ge \min\{3^6, 2^{10}\} = 3^6$, thus $10.28 < 2^{-1/3}81 - 54 \le c_pq^{2/3} - 2\sqrt{q}$. $\square$

RESULT 1.5.10 (Blokhuis–Lovász–Storme–Szőnyi [22]). *Let $\mathcal{B}$ be a minimal t-fold blocking set in* $\mathrm{PG}(2,q)$*,* $q = p^h$*,* $h \geq 1$*,* $|\mathcal{B}| = t(q+1)+s$*,* $s+t < (q+3)/2$*. Then every line intersects $\mathcal{B}$ in $t \pmod p$ points.*

DEFINITION 1.5.11. *A* weighted point-set *is a set of points $\mathcal{B}$ with a weight function $w\colon \mathcal{B} \to \mathbb{N}$. The* size *of $\mathcal{B}$ is defined as $|\mathcal{B}| = \sum_{P\in\mathcal{B}} w(P)$. A weighted point-set $\mathcal{B}$ (with weight w) in $\Pi_q = (\mathcal{P},\mathcal{L})$ is a* t-fold weighted blocking set *if $\sum_{P\in\ell} w(P) \geq t$ for all $\ell \in \mathcal{L}$.*

Multiple weighted covering sets are defined analogously. Weighted blocking sets were studied, e.g., in [38] and [19]. In such context, the sum of some point-sets is a weighted set in which the weight of a point P is the number of sets in the sum in which P is contained. We will need the following results.

RESULT 1.5.12. ([38], Theorems 2.5, 2.13 and Proposition 2.15) *Let $\mathcal{B}$ be a weighted k-fold blocking set in* $\mathrm{PG}(2,p)$*, p prime, with $|\mathcal{B}| = kp+k+r$, $k+r < (p+2)/2$. Then $\mathcal{B}$ contains the sum of k (not necessarily different) lines (considered as point-sets).*

RESULT 1.5.13. ([19], Theorem 3.10) *Let $\mathcal{B}$ be a weighted k-fold blocking set in* $\mathrm{PG}(2,q)$*, $q = p^h$, p prime, $h > 1$. Let $c_2 = c_3 = 2^{-1/3}$ and $c_p = 1$ for $p > 3$. Assume that $|\mathcal{B}| = kq+k+c-(k-1)(k-2)/2$, where*

(1) $c < c_p q^{2/3}$ and $k < \min\{c_p q^{1/6}, q^{1/4}/2\}$, or

(2) $q = p^2$, $k < q^{1/4}/2$ and $c < q^{3/4}/2$.

If the number of simple points (i.e., points with weight one) is at least $(k-2)(q+\sqrt{q}+1)+16\sqrt{q}+8q^{1/4}$ in (1) and at least $(k-2)(q+\sqrt{q}+1)+16\sqrt{q}+16q^{1/6}$ in (2), then $\mathcal{B}$ contains the sum of the point-sets of k (not necessarily different) Baer subplanes and/or lines (considered as point-sets).

Ovals, (k,n)-arcs and unitals

DEFINITION 1.5.14. *A point-set $\mathcal{K}$ of size k in $\Pi_q = (\mathcal{P},\mathcal{L})$ is a* (k,n)-arc *if $|\ell \cap \mathcal{K}| \leq n$ for all $\ell \in \mathcal{L}$. The term k-arc is also used to denote a $(k,2)$-arc. An* oval *and a* hyperoval *is a $(q+1)$-arc and a $(q+2)$-arc, respectively.*

Note that it is common to ensure the existence of an n-secant line in the definition of a (k,n)-arc, yet we do not require it. A non-degenerate conic is an oval in $\mathrm{PG}(2,q)$. If q is even, then any oval in Π_q can be extended to a hyperoval.

The dual of a (hyper)oval is called a *dual (hyper)oval.* For convenience, 2-secant lines of an arc are shortly called secants.

An oval $\mathcal{O}$ of $\Pi_q = (\mathcal{P}, \mathcal{L})$ has one tangent in each of its points. If q is odd, then a point not on $\mathcal{O}$ is incident with either zero or two tangents to $\mathcal{O}$, and it is called an inner (internal) or an outer (external) point of $\mathcal{O}$, respectively. We denote by $\mathrm{Inn}(\mathcal{O})$, $\mathrm{Out}(\mathcal{O})$, $\mathrm{Skw}(\mathcal{O})$, $\mathrm{Tan}(\mathcal{O})$, $\mathrm{Sec}(\mathcal{O})$ the set of inner points and outer points of $\mathcal{O}$, and the set of skew lines, tangents lines and secant lines to $\mathcal{O}$, respectively. If $P \notin \mathcal{O}$, then $|P \cap \mathrm{Skw}(\mathcal{O})| = |P \cap \mathrm{Sec}(\mathcal{O})|$, and dually, if $\ell \notin \mathrm{Tan}(\mathcal{O})$, then $|\ell \cap \mathrm{Inn}(\mathcal{O})| = |\ell \cap \mathrm{Out}(\mathcal{O})|$. It is easy to compute that $|\mathrm{Out}(\mathcal{O})| = |\mathrm{Sec}(\mathcal{O})| = q(q+1)/2$ and $|\mathrm{Inn}(\mathcal{O})| = |\mathrm{Skw}(\mathcal{O})| = q(q-1)/2$.

Looking around from a point of a (k,n)-arc we see that $k \leq 1+(q+1)(n-1)$; in case of equality the arc is called a maximal (k,n)-arc. Every line intersects such an arc in either zero or n points.

RESULT 1.5.15 (Denniston [33], Ball–Blokhuis–Mazzocca [14]). *Let* $1 < n < q$. *Then a maximal* (k,n)*-arc exists in* $\mathrm{PG}(2,q)$ *if and only if* $n \mid q$ *and* q *is even.*

DEFINITION 1.5.16. *A* unital *in* Π_q*,* q *a square, is a set of* $q\sqrt{q}+1$ *points which intersects every line in* 1 *or* $\sqrt{q}+1$ *points.*

In $\mathrm{PG}(2,q)$, q a square, Hermitian curves are unitals. Let $\mathcal{U}$ be a unital in a projective plane of order q. By looking around from a point of $\mathcal{U}$ and then from a point not in $\mathcal{U}$, we easily see that there is exactly one tangent to $\mathcal{U}$ at any point of $\mathcal{U}$, and that there are $\sqrt{q}+1$ tangents to $\mathcal{U}$ through any point not in $\mathcal{U}$. Thus the total number of tangents and $(\sqrt{q}+1)$-secants of $\mathcal{U}$ is $q\sqrt{q}+1$ and $q(q-\sqrt{q}+1)$, respectively.

For more information and details about the above structures we refer to [46].

Chapter 2

Results on multiple blocking sets

2.1 Some properties of multiple blocking sets in $\mathrm{PG}(2,q)$

THEOREM 2.1.1 ([B]). *Let $\mathcal{S}$ be a t-fold blocking set in* $\mathrm{PG}(2,q)$*,* $|\mathcal{S}| = t(q+1)+k$*. Then there are at least $q+1-k-t$ distinct t-secants to $\mathcal{S}$ through any essential point of $\mathcal{S}$.*

Proof. Let $P \in \mathcal{S}$ be essential, and let ℓ be an arbitrary t-secant of $\mathcal{S}$ that is not incident with P. Assume that there are less than $(q+1-k-t)$ t-secants through P. We claim that in this case every t-secant through P intersects ℓ in a point of $\ell \cap \mathcal{S}$. Having proved this, we easily get a contradiction: since P is essential, there exists a line e through P that is a t-secant. Choose a point $Q \in e \setminus \mathcal{S}$. If the only t-secant through Q is e, then $|\mathcal{S}| \geq t(q+1)+q$ and the statement of the Lemma is trivial. Thus we may assume that there is another t-secant, say ℓ^*, through Q. But by our claim every t-secant through P intersects ℓ^* in a point of $\ell^* \cap \mathcal{S}$, which is a contradiction, since $e \cap \ell^* = Q \notin \mathcal{S}$. So now we have to prove the claim above.

Choose a coordinate system in such a way that the common point of the vertical lines, (∞) is in $\mathcal{S}$, and ℓ is the line at infinity.

Suppose that $\mathcal{S} \cap \ell = \{(\infty)\} \cup \{(1 : m_i : 0) \mid i = 1, \ldots, t-1\}$. Let $\mathcal{S} \setminus \ell = \{(x_i, y_i) \mid i = 1, \ldots, tq+k\} \subset \mathrm{AG}(2,q) = \mathrm{PG}(2,q) \setminus \ell$. We may assume that $P = (x_1, y_1)$. Let $H(B,M)$ be the Rédei polynomial of $\mathcal{S} \setminus \{(\infty)\}$; that is, let

$$H(B,M) = \prod_{i=1}^{t-1}(M - m_i) \cdot \prod_{i=1}^{tq+k}(B + x_i M - y_i).$$

Note that $\deg_{B,M} H(B,M) = t(q+1)+k-1$. A line with slope m and y-intersection b (defined by the equation $Y = mX + b$) intersects $\mathcal{S}$ in exactly as many points as the number of (linear) factors vanishing in $H(b,m)$; that is, the multiplicity of the root b of the one-variable polynomial $H(B,m)$, or the multiplicity of the root m of $H(b,M)$, provided that these one-variable polynomials are not identically zero. This latter phenomenon occurs iff we substitute $M = m_i$ for some $i = 1, \ldots, t-1$.

Since $\mathcal{S}$ is a t-fold blocking set, every pair (b,m) produces at least t factors vanishing in H; thus by the multiplicity version of Alon's Combinatorial Nullstellensatz (Result 1.1.2; or, regarding this special case, see [27] or [22]), $H(B,M)$ can be written in the form

$$(B^q-B)^t F_0(B,M)+(B^q-B)^{t-1}(M^q-M)F_1(B,M)+\ldots+(M^q-M)^t F_t(B,M),$$

where $\deg(F_i) \le k+t-1$. Since $\prod_{i=1}^{t-1}(M-m_i)$ divides $H(B,M)$ and $(M^q-M) = \prod_{m\in \mathrm{GF}(q)}(M-m)$, $\prod_{i=1}^{t-1}(M-m_i)$ divides $F_0(B,M)$ as well. Let $F_0^*(B,M) = F_0(B,M)/\prod_{i=1}^{t-1}(M-m_i)$. Fix $m \in \mathrm{GF}(q)\setminus\{m_i\colon i=1,\ldots,t-1\}$. Then $F_0(B,m)$ and $F_0^*(B,m)$ differ only in a nonzero constant multiplier; $0 \not\equiv H(B,m) = (B^q - B)^t F_0(B,m)$; and $\deg_B F_0(B,m) \le k$. If a line $Y = mX+b$ intersects $\mathcal{S}$ in more than t points, then the multiplicity of the root b of $H(B,m)$ is more than t, thus $(B-b)$ divides $F_0^*(B,m)$. Conversely, if $F_0^*(b,m) = 0$, then the line $Y = mX+b$ intersects $\mathcal{S}$ in more than t points.

If there are less than $(q+1-k-t)$ t-secants through $P = (x_1,y_1)$, then there are more than k non-vertical ($>t$)-secants through P with slopes different from m_i, $i = 1,\ldots,t-1$. Hence there are more than k pairs (b,m) for which $b+mx_1-y_1 = 0$ and $F_0^*(b,m) = 0$; in other words, the algebraic curves defined by $B+Mx_1-y_1 = 0$ and $F_0(B,M) = 0$ have more than k points in common. Since $\deg_{B,M} F_0^*(B,M) \le k$, this implies that $B+Mx_1-y_1 \mid F_0^*(B,M)$ (e.g., by Bezout's theorem). Geometrically this means that every line passing through $P = (x_1,y_1)$ not through $\mathcal{S}\cap\ell$ are ($>t$)-secants of $\mathcal{S}$. □

REMARK 2.1.2. *Theorem 2.1.1 is similar to Lemma 2.3 in [22]. The proof given there works for* $k+t < (q+3)/2$ *(although it is only stated implicitly before the Lemma) and it gives a somewhat better result, that there are at least* $(q-k)$ *t-secants through every essential point.*

COROLLARY 2.1.3 ([B]). *Let $\mathcal{B}$ be a t-fold blocking set in* $\mathrm{PG}(2,q)$ *with* $|\mathcal{B}| \le (t+1)q$ *points. Then there is exactly one minimal t-fold blocking set in $\mathcal{B}$, namely the set of essential points of $\mathcal{B}$.*

Proof. Let $\mathcal{B}'$ be a minimal t-fold blocking set of size $t(q+1)+k'$ inside $\mathcal{B}$, and let $P \in \mathcal{B}'$. Then P is an essential point of $\mathcal{B}'$, hence there are at least $q+1-k'-t$ t-secants to $\mathcal{B}'$ through P. At least $q+1-k'-t-(|\mathcal{B}|-|\mathcal{B}'|) \geq 1$ of these must be a t-secant to $\mathcal{B}$ as well, thus P is an essential point of $\mathcal{B}$. On the other hand, all essential points of $\mathcal{B}$ must be in $\mathcal{B}'$. □

REMARK 2.1.4. *The case $t = 1$ of the above corollary was already proved by Szőnyi [70]. Recently, Harrach [44] proved a more general result for weighted multiple blocking sets in higher dimensional projective spaces. For non-weighted t-fold blocking sets in* PG$(2,q)$*, Harrach's result is the same as Corollary 2.1.3.*

Harrach pointed out the following in [44]. For blocking sets (i.e., $t = 1$), this connection can also be found in [21] and [70].

REMARK 2.1.5. *Corollary 2.1.3 is equivalent with Theorem 2.1.1.*

Proof. Suppose that Corollary 2.1.3 holds. Let $\mathcal{S}$ be a minimal t-fold blocking set with $|\mathcal{S}| = t(q+1)+k \leq (t+1)q$. Should there be a point $P \in \mathcal{S}$ with $s < q+1-k-t$ t-secants through it, add one new point P_i to $\mathcal{S}$ on each of the t-secants through P, $1 \leq i \leq s$. Then the extended set $\mathcal{S}'$ is a t-fold blocking set and $|\mathcal{S}'| \leq (t+1)q$. Note that $\mathcal{S}' \setminus \{P\}$ is also a t-fold blocking set, hence it contains a minimal t-fold blocking set that is different from $\mathcal{S}$. Thus $\mathcal{S}'$ would violate Corollary 2.1.3, a contradiction. □

Remarks 2.1.4 and 2.1.5 show that Theorem 2.1.1 also follows from the recent results of Harrach [44]. However, the proof of Theorem 2.1.1 given here is a basically self-contained application of the polynomial method.

Next we characterize a somewhat artificially looking type of blocking sets. The motivation of the upcoming theorem is found in Chapter 3, Section 3.3.

LEMMA 2.1.6 ([E]). *Let q be a power of the prime p, and let $\mathcal{L}$ be a set of non-vertical lines of* AG$(2,q)$ *which cover every point of* AG$(2,q)$ *exactly k times ($k \geq 1$) except possibly the points of ν fixed vertical lines, where $\nu(k+1) \leq q$ and $\nu k < p$. Then $\mathcal{L}$ consists of the union of k parallel classes, or $\mathcal{L}$ consists of the kq non-vertical lines passing through k fixed points on a fixed vertical line.*

Proof. Counting the lines of $\mathcal{L}$ through the points of a non-exceptional vertical line we see that $|\mathcal{L}| = kq$. Suppose $\nu = 0$. Fix an arbitrary line $\ell \in \mathcal{L}$, and consider AG$(2,q)$ embedded into PG$(2,q)$ (and also extend the lines by their ideal points). As the affine points of ℓ are covered exactly k times by $\mathcal{L}$, there are $kq - q(k-1) = q$ lines of $\mathcal{L}$ incident with the ideal point of ℓ, whence the statement follows.

Suppose $\nu \geq 1$. Since the lines of $\mathcal{L}$ are non-vertical, they are given by the equations $Y + m_i X + b_i = 0$, where $m_i, b_i \in \mathrm{GF}(q)$, $i \in \{1, \ldots, kq\}$. Consider the following dual Rédei polynomial (over $\mathrm{GF}(q)$):

$$f(X,Y) = \prod_{i=1}^{kq} (Y + m_i X + b_i).$$

Then $\deg_{X,Y} f = kq$. Let $S \subset \mathrm{GF}(q)$ be the subset of $q - \nu$ elements x for which on the vertical line $X = x$ every point is covered exactly k-times. Consider the polynomial

$$g(X) = \prod_{x \in S} (X - x).$$

Then $\deg_X g = q - \nu$. The elements of $S \times \mathrm{GF}(q)$ are zeros of $f(X,Y)$ with multiplicity k, thus by the multiplicity version of Alon's Combinatorial Nullstellensatz we get

$$f(X,Y) = (Y^q - Y)^k + \ldots + f_i(X,Y)(Y^q - Y)^{k-i} g(X)^i + \ldots + f_k(X,Y) g(X)^k,$$

where $\deg_{X,Y} f_i \leq kq - q(k-i) - (q-\nu)i = i\nu$ for all $1 \leq i \leq k$. For convenience, let $f_0(X,Y) \equiv 1$. Fix an arbitrary $x \notin S$. Then $g(x) \neq 0$, and including the arising constants into the f_is we get

$$f(x,Y) = (Y^q - Y)^k + f_1(x,Y)(Y^q - Y)^{k-1} + \ldots + f_k(x,Y).$$

Note that since the multiplicity of the root y is the number of lines of $\mathcal{L}$ passing through $(x,y) \in \mathrm{AG}(2,q)$, no root of $f(x,Y)$ can have multiplicity larger than q.

Now let h be the largest integer for which $f_h(x,Y) \not\equiv 0$ $(0 \leq h \leq k)$. Then

$$f(x,Y) = (Y^q - Y)^k + f_1(x,Y)(Y^q - Y)^{k-1} + \ldots + f_h(x,Y)(Y^q - Y)^{k-h}.$$

Consider

$$f^*(x,Y) = \frac{f(x,Y)}{(Y^q - Y)^{k-h}} = (Y^q - Y)^h + (Y^q - Y)^{h-1} f_1(x,Y) + \ldots + f_h(x,Y).$$

Let R denote the set of distinct roots of $f^*(x,Y)$. Then $r(y) = \prod_{y \in R}(Y - y)$ divides $Y^q - Y$, and hence $f_h(x,Y)$ as well. Thus $|R| \leq \deg f_h(x,Y) \leq h\nu$. Let $'$ denote the derivation in the variable Y. As every root of $f^*(x,Y)$ is root of $f^{*\prime}(x,Y)$ with one less multiplicity, $\deg_Y f^{*\prime}(x,Y) \geq \deg_Y f^*(x,Y) - |R| \geq hq - h\nu \geq hq - k\nu$ holds except if $f^{*\prime}(x,Y) \equiv 0$. On the other hand,

$$f^{*\prime}(x,Y) = -h(Y^q-Y)^{h-1}+f_1'(x,Y)(Y^q-Y)^{h-1}-(h-1)f_1(x,Y)(Y^q-Y)^{h-2}+\dots$$

$$\dots - f_{h-1}(x,Y) + f_h'(x,Y),$$

and since $\deg f_i' < i\nu$, then $\deg f^{*\prime} < \max\{i\nu+(h-i)q\colon 0 \leq i \leq h\} \leq (h-1)q+\nu$. As $\nu(k+1) \leq q$, $hq-k\nu < (h-1)q+\nu$ can not hold. Thus $f^{*\prime} \equiv 0$, which means that $f^*(x,Y) \in \mathrm{GF}(q)[Y^p]$. Using the binomial expansion, we see that the terms of $f^*(x,Y)$ are of form Y^{qi+j} where $0 \leq i \leq k-h$ and $0 \leq j \leq h\nu \leq k\nu < p$, thus only $j=0$ occurs. This means that

$$f^*(x,Y) = Y^{hq} + a_1 Y^{(h-1)q} + \dots + a_h$$

with proper $a_i \in \mathrm{GF}(q)$ (i.e., $f^*(x,Y) \in \mathrm{GF}(q)[Y^q]$ and it has degree h). Since $y^q = y$ for every $y \in \mathrm{GF}(q)$, $f^*(x,Y)$ may have only h different zeros. Nevertheless, $f^*(x,Y)$ is fully reducible, so it has hq zeros altogether (summing up the multiplicities), but each distinct zero has multiplicity at most $q-k+h$. Therefore $hq \leq h(q-k+h)$. This can only happen if $h=0$ or $h=k$. In the first case $f(x,Y) = (Y^q-Y)^k$ by the definition of h, thus every point on the line $X=x$ is covered exactly k-times, while in the latter case $f(x,Y) = f^*(x,Y) \in \mathrm{GF}(q)[Y^q]$ and we find k points on the vertical line $X=x$ that are covered q-times. Thus the lemma is proved. □

REMARK 2.1.7. *Note that the two possibilities on the structure of the set of lines in the above lemma are essentially the same: if we view* AG$(2,q)$ *inside* PG$(2,q)$, *then we see that our line-set consists of the lines intersecting a fixed line ℓ in one of k fixed points. This line ℓ may be the line at infinity or an affine line as well.*

A condition like $\nu k < p$ is necessary: if we take a Baer subplane $B = (\mathcal{P}_0, \mathcal{L}_0)$ in PG$(2,q)$, $q=p^2$, so that $(\infty) \in \ell_\infty$ is a flag of it, then $\mathcal{P}_0 \cap \mathrm{AG}(2,q)$ is covered by the $\nu = \sqrt{q} = p$ affine lines of B incident with (∞). Thus if $\mathcal{L}$ is the set of the non-vertical affine lines of B, then all other points of AG$(2,q)$ are covered exactly $k=1$ times by $\mathcal{L}$. Thus $\mathcal{L}$ is an example in which $\nu k = p$, and the conclusion of Theorem 2.1.6 fails.

REMARK 2.1.8. *A similar result can be obtained using known results on weighted multiple blocking sets in the following way. Give weight k to the ν exceptional vertical lines and to the line at infinity to obtain a weighted line-set $\mathcal{L}^*$ of size*

$kq+(\nu+1)k$. Then $\mathcal{L}^*$ is a weighted k-fold covering set, hence we may apply the dual of Results 1.5.12 and 1.5.13. If $q=p$, to apply Result 1.5.12, we need $(\nu+1)k<(p+2)/2$. Provided so, $\mathcal{L}^*$ contains the sum of k points $P_1,\dots,P_k$ (considered as line-sets). Note that $(\infty)\neq P_i$ as only $\nu<p$ vertical lines are included in $\mathcal{L}^*$. A line $P_i\cap P_j$ has weight more than one, hence it must be an exceptional line, which lines do not have an intersection point besides (∞), hence $P_i\cap P_j$ is the same line for all $1\le i<j\le k$. Thus in $\mathrm{AG}(2,p)$ we obtain the same result under the somewhat stricter condition $(\nu+1)k<(p+2)/2$. In $\mathrm{AG}(2,p^h)$, $h>1$, we may apply Result 1.5.13 if its somewhat technical conditions hold (in particular, in case of $h=2$, Result 1.5.13 requires $k<\sqrt[4]{q}/2=\sqrt{p}/2$, while for $h\ge 3$ it also needs $k<c_p\sqrt[6]{q}$, which are further restrictions on k if $h<6$). Provided so, we may conclude that $\mathcal{L}^*$ contains the sum of k points or line-sets of Baer subplanes. If $\nu<\sqrt{q}$, then Baer subplanes cannot be involved, as such a line-set would cover all the points of the Baer subplane $\sqrt{q}+1>k$ times, but the affine points of a Baer subplane cannot be covered by the $\nu<\sqrt{q}$ exceptional vertical lines. Thus under these assumptions we obtain the same conclusion as in Lemma 2.1.6. However, if h is large enough, the assumptions of Result 1.5.13 are less restrictive than those of Lemma 2.1.6.

2.2 Two disjoint blocking sets in $\mathrm{PG}(2,q)$

Next we construct two small disjoint blocking sets in $\mathrm{PG}(2,q)$ in order to find a small double blocking set. No such general constructions were known if q is not a square; we give the related results at the end of the section. We prove the following theorem.

THEOREM 2.2.1 ([B]). *Let $h\ge 3$ odd, $\alpha\ge 1$ an integer, p an odd prime, $r=p^\alpha$, $q=r^h$. Then there exist two disjoint blocking sets of size $q+(q-1)/(r-1)$ in $\mathrm{PG}(2,q)$. Consequently, $\tau_2(\mathrm{PG}(2,q))\le 2(q+(q-1)/(r-1))$.*

As there are two disjoint Baer subplanes in $\mathrm{PG}(2,q)$ if q is a square, we immediately get the following result.

COROLLARY 2.2.2 ([B]). *Let r denote the order of the largest proper subfield of $\mathrm{GF}(q)$, where q is odd (not a prime), or q is a square. Then there exist two disjoint blocking sets of size $q+(q-1)/(r-1)$ in $\mathrm{PG}(2,q)$, and so $\tau_2(\mathrm{PG}(2,q))\le 2(q+(q-1)/(r-1))$.*

Throughout this section GF(q) denotes the finite field of $q = r^h$ elements of characteristic p, $r = p^\alpha$.

Let $f\colon \mathrm{GF}(q) \to \mathrm{GF}(q)$, and consider its graph $\mathcal{U}_f = \{(x : f(x) : 1)\colon x \in \mathrm{GF}(q)\}$ in the affine plane AG$(2,q)$. The slopes (or directions) determined by $\mathcal{U}_f$ is the set $S_f = \{(f(x) - f(y))/(x - y)\colon x, y \in \mathrm{GF}(q), x \neq y\}$. It is well-known that $\mathcal{U}_f \cup \{(1 : m : 0)\colon m \in S_f\}$ is a blocking set in PG$(2,q)$. This blocking set has the property that there is a line such that there are precisely q points in the blocking set not on this line. Such blocking sets are called blocking sets of Rédei type. For more information about these we refer to [41].

Let γ be a primitive element of GF$(q)^*$, the multiplicative group of GF(q). Let $d \mid q-1$, $m = (q-1)/d$, and let $D = \{x^d\colon x \in \mathrm{GF}(q)^*\} = \{\gamma^{kd}\colon 0 \le k < m\}$. Let $1 \le t \le m-1$. Then $\gamma^{dt} \neq 1$. On the other hand, $\sum_{c \in D} c^t = \sum_{c\in D} c^t \gamma^{dt}$, therefore $\sum_{c\in D} c^t = 0$ follows.

First we copy the ideas of the proof of the Hermite–Dickson theorem on permutation polynomials from [57] to prove a generalization of it to multiplicative subgroups of GF$(q)^*$.

LEMMA 2.2.3 ([B]). *Let* GF(q) *be a field of characteristic* p, $d \mid q-1$, $m = (q-1)/d$. *Let* $D = \{x^d\colon x \in \mathrm{GF}(q)^*\}$ *be the set of nonzero* d^{th} *powers. Let* $a_1, \dots, a_m$ *be a sequence of elements of* D. *Then the following two conditions are equivalent:*

(i) $a_1, \dots, a_m$ *are pairwise distinct;*

(ii) $\sum_{i=1}^m a_i^t = 0$ *for all* $1 \le t \le m-1$, $p \nmid t$.

Proof. Let γ be a primitive element of GF$(q)^*$. Then $a_i = \gamma^{\alpha_i d}$ for appropriate $\alpha_i \in \mathbb{N}$. Let $g_i(x) = \sum_{j=0}^{m-1} a_i^{m-j} x^j$. Choose $b = \gamma^{\beta d} \in D$. Then $g_i(b)$ equals

$$\sum_{j=0}^{m-1} \gamma^{\alpha_i(m-j)d}\gamma^{d\beta j} = \sum_{j=0}^{m-1} \gamma^{\alpha_i m d}\gamma^{d(\beta-\alpha_i)j} = \sum_{j=0}^{m-1} (\gamma^{jd})^{\beta-\alpha_i} = \begin{cases} m, \text{ if } \beta - \alpha_i = 0, \\ 0 \text{ otherwise.} \end{cases}$$

As $m \mid (q-1)$, $m \not\equiv 0 \pmod p$. Let

$$g(x) = \sum_{i=1}^m g_i(x) = \sum_{j=0}^{m-1} \left(\sum_{i=1}^m a_i^{m-j} \right) x^j.$$

Then $\deg g(x) < m$, and $g(b) = |\{i \in \{1, \dots, m\}\colon a_i = b\}| \cdot m \pmod p$. Thus $a_1, \dots, a_m$ are pairwise distinct $\iff$ $g(b) = m$ for all $b \in D$ $\iff$ $g(x) \equiv m$ $\iff$ $\sum_{i=1}^m a_i^t = 0$ for all $1 \le t \le m-1$. As $x \mapsto x^p$ is an automorphism of GF(q), the statement follows. □

THEOREM 2.2.4 ([B]). *Let* $\mathrm{GF}(q)$ *be a field of characteristic* p, $m \mid q-1$, *and let* D *be the multiplicative subgroup of* $\mathrm{GF}(q)^*$ *of* m *elements. Let* $g \in \mathrm{GF}(q)[x]$ *be a polynomial such that* $g(b) \in D$ *for all* $b \in D$. *Then* $g|_D\colon D \to D$ *is a permutation of* D *if and only if the constant term of* $g(x)^t \pmod{(x^m-1)}$ *is zero for all* $1 \le t \le m-1$, $p \not| \, t$.

Proof. Let $b \in D$. If $b \neq 1$, then $b^{m-1} + b^{m-2} + \ldots + b + 1 = (b^m-1)/(b-1) = 0$, otherwise it equals m. Let $g^{[t]}(x) = g(x)^t \pmod{(x^m-1)}$. As $g(x)^t$ and $g^{[t]}(x)$ take the same values on D and $\deg g^{[t]}(x) < |D|$, by interpolation we have $g^{[t]}(x) = \sum_{b\in D} \frac{g^t(b)}{m}\left(\left(\frac{x}{b}\right)^{m-1} + \ldots + \frac{x}{b} + 1\right)$. Thus the constant term of $g^{[t]}(x)$ is $\sum_{b\in D} g^t(b)$, hence Lemma 2.2.3 yields the stated result. □

COROLLARY 2.2.5 ([B]). *Let* $D \le \mathrm{GF}(q)^*$ *be a multiplicative subgroup of* m *elements. Suppose that* $g \in \mathrm{GF}(q)[x]$ *maps a coset* c_1D *into another coset* c_2D. *Then this mapping is bijective if and only if the constant term of* $g(c_1x)^t \pmod{(x^m-1)}$ *is zero for all* $1 \le t \le m-1$, $p \not| \, t$.

Proof. Apply Theorem 2.2.4 to $g^*(x) = c_2^{-1}g(c_1x)$. □

Now we are ready to prove Theorem 2.2.1. Recall that $q = r^h$, $h \ge 3$ odd, $r = p^\alpha$, $\alpha \ge 1$, p an odd prime.

Proof of Theorem 2.2.1 ([B]). Let $f, g\colon \mathrm{GF}(q) \to \mathrm{GF}(q)$ be two additive functions. Then the set of directions determined by f is $\{(f(x)-f(y))/(x-y)\colon x \neq y \in \mathrm{GF}(q)\} = \{f(x)/x\colon x \in \mathrm{GF}(q)^*\}$, and these correspond to the points $(1 : f(x)/x : 0) = (x : f(x) : 0)$ on the line at infinity. The analogous assertion holds for g as well. Note that interchanging the second and third coordinates is an automorphism of $\mathrm{PG}(2,q)$. Consider the following blocking sets:

$$\mathcal{B}_1 = \underbrace{\{(x : f(x) : 1)\}}_{\mathcal{U}_1} \cup \underbrace{\{(x : f(x) : 0)\}_{x\neq 0}}_{\mathcal{D}_1},$$

$$\mathcal{B}_2 = \underbrace{\{(y : 1 : g(y))\}}_{\mathcal{U}_2} \cup \underbrace{\{(y : 0 : g(y))\}_{y\neq 0}}_{\mathcal{D}_2}.$$

Besides additivity, suppose that g is an automorphism of $\mathrm{GF}(q)$ and that $f(x) = 0 \iff x = 0$. The latter assumption yields $(0 : 0 : 1) \notin \mathcal{D}_2$, so $\mathcal{D}_2 \cap \mathcal{B}_1$ is empty. If $(x : f(x) : 0) = (y : 1 : g(y)) \in \mathcal{D}_1 \cap \mathcal{U}_2$, then $g(y) = 0$, hence $y = 0$ and $x = 0$, a contradiction. Thus $\mathcal{D}_1 \cap \mathcal{U}_2$ is also empty. Now we need $\mathcal{U}_1 \cap \mathcal{U}_2 = \emptyset$. Suppose that $(y : 1 : g(y)) = (x : f(x) : 1)$. Then $x \neq 0$

(otherwise $y = g(y) = 0 \neq 1$), thus $(y : 1 : g(y)) = (x/f(x) : 1 : 1/f(x))$, so $g(x/f(x)) = 1/f(x)$. As g is multiplicative, this yields $g(x)f(x) = g(f(x))$ $(\star)$. We want this equation to have no solutions in GF$(q)^*$.

Let D be the set of nonzero $(r-1)^{\text{th}}$ powers, $m = (q-1)/(r-1) = r^{h-1} + \ldots + r + 1$. Then m is odd. Let $g(x) = x^r$ and $f(x) = \frac{1}{a}(x^r + x)$, $a \in$ GF$(q)^*$. Then g is an automorphism and f is additive. Moreover, if $x \neq 0$, then $f(x) = \frac{1}{a}x(x^{r-1}+1)$ is zero iff $x^{r-1} = -1$, consequently $1 = x^{m(r-1)} = (-1)^m = -1$ as m is odd, which is impossible in odd characteristic. Hence $f(x) = 0 \iff x = 0$. It is easy to see that $f(x)/x = f(y)/y$ if and only if $(x/y)^{r-1} = 1$, thus $|\mathcal{D}_1| = (q-1)/(r-1)$; similarly, $|\mathcal{D}_2| = (q-1)/(r-1)$ as well.

Equality $(\star)$ now says $x^r = (\frac{1}{a}(x^r + x))^{r-1} = \frac{x^{r-1}}{a^{r-1}}(x^{r-1}+1)^{r-1}$, equivalently

$$a^{r-1} = \frac{(x^{r-1}+1)^{r-1}}{x} =: \psi^*(x). \tag{2.1}$$

Recall that we want (2.1) to have no solutions in GF$(q)^*$. To this end we need to find an $(r-1)^{\text{th}}$ power (i.e., an element of D) that is not in the range of ψ^*. Note that $\psi^*(b) \in D \iff b \in D$. Let $\psi(x) = (x^{r-1}+1)^{r-1}x^{q-2}$. Then $\psi^*(x)$ and $\psi(x)$ take the same values on GF$(q)^*$. Thus we need to show that $\psi|_D$ does not permute D. By Theorem 2.2.4, it is enough to show that the constant term of $\psi^{r-1}(x) \pmod{(x^m - 1)}$ is not zero.

Consider

$$\psi^{r-1}(x) = \sum_{k=0}^{(r-1)^2} \binom{(r-1)^2}{k} x^{k(r-1)+(r-1)(q-2)}.$$

Since $k(r-1) + (r-1)(q-2) \equiv (k-1)(r-1) \pmod{m}$, the exponents reduced to zero have $k = 1 + \ell\frac{m}{\gcd(m,r-1)}$ for some $\ell \geq 0$. As $\binom{(r-1)^2}{1} \equiv 1 \pmod{p}$, it is enough to show that $\binom{(r-1)^2}{k} \equiv 0 \pmod{p}$ for the other possible values of k.

As $0 \leq k \leq (r-1)^2$, $m/\gcd(m, r-1) \geq r^2$ would imply that $\ell \geq 1$ does not occur. By $m/\gcd(m, r-1) > m/r > r^{h-2}$, this is the case for $h \geq 5$; and also for $h = 3$ and $r \not\equiv 1 \pmod{3}$, as in this case $m = r^2 + r + 1$ and $\gcd(m, r-1) = \gcd(3, r-1) = 1$.

Now suppose $h = 3$, $r \equiv 1 \pmod{3}$. Then $1 \leq \ell \leq 2$, and so $k = 1 + \ell m/\gcd(m, r-1) = 1 + \ell(r^2+r+1)/3 \equiv (3+\ell)/3 \not\equiv 0, 1 \pmod{r}$ as $r > 5$. Let $k! = p^\beta k'$, where $\gcd(k', p) = 1$. Consider the product $\pi = (r^2 - 2r - 1)\ldots(r^2 - 2r + 2 - k)(r^2 - 2r + 1 - k)(r^2 - 2r - k)$. As $\binom{r^2-2r-1}{k}$ is an integer, $k! \mid \pi$, so $p^\beta \mid \pi$. Since $(r^2 - 2r + 1)(r^2 - 2r)$ is divisible by r, but $(r^2 - 2r + 1 - k)(r^2 - 2r - k)$ is not, $p^{\beta+1}$ divides $(r^2 - 2r + 1)\ldots(r^2 - 2r + 2 - k)$, hence $\binom{(r-1)^2}{k} \equiv 0 \pmod{p}$. Thus the proof is finished. $\square$

Let us mention some results in connection with Theorem 2.2.1. As the union of two disjoint blocking sets, a double blocking set of size $2q+2q^{2/3}+2q^{1/3}+2$ was constructed by Davydov, Giulietti, Marcugini and Pambianco [32] in $\mathrm{PG}(2, q = p^3)$ for $p \leq 73$, p prime, and by Polverino and Storme ([62], cited in [22]) in $\mathrm{PG}(2, q = p^{3h})$ for $p^h \equiv 2 \pmod 7$. Note that Result 1.5.8 roughly says that a double blocking set in $\mathrm{PG}(2, q)$ of size at most $2q + q^{2/3}$ contains the union of two disjoint Baer subplanes. These examples show that the term $q^{2/3}$ is of the right magnitude if q is a cube.

Also, according to [67], the PhD thesis of Van de Voorde [74] implicitly contains the following general result: if B is a minimal blocking set in $\mathrm{PG}(2, q)$, $q = p^h$, that is not a line, and $|B| \leq 3(q - p^{h-1})/2$, then there is a small $\mathrm{GF}(p)$-linear blocking set that is disjoint from B. It seems that the proof requires the characteristic of the field to be more than five. Note that this implies $\tau_2 \leq 2q + q/p + (q-1)/(p-1) + 1$. For an overview of linear sets, we refer to [61]. We remark that the functions f and g in the above construction are both linear over $\mathrm{GF}(r)$, and hence the arising blocking sets are linear as well.

Finally, let us note that two specific disjoint linear sets were also presented in [15] in order to construct semifields. The rank of those are different from what we need if we want to obtain two disjoint linear blocking sets. However, the construction probably can be modified so that one may use it to find two disjoint blocking sets.

2.3 Lower bound on the size of multiple blocking sets

The next theorem was originally proved by Ball in [12] using basically the same counting arguments, though in a less friendly way. Note that for $t = 1$, a Baer subplane proves the theorem sharp. Using this formulation, a slight improvement is easily achieved for $t \geq 2$ as we mention in Remark 2.3.2.

RESULT 2.3.1 (Ball [12]). *Let $\mathcal{B}$ be a t-fold blocking set in an arbitrary projective plane of order q that contains no line,* $1 \leq t \leq q-2$. *Then*

$$|\mathcal{B}| \geq tq + \sqrt{tq} + 1.$$

Proof. Suppose that there exists a line ℓ that intersects $\mathcal{B}$ in at least x points. Since $\ell \not\subset \mathcal{B}$, $x \leq q$ and there is a point $P \in \ell \setminus B$. Then counting the number of points on the lines through P we get that $|\mathcal{B}| \geq tq + x$. Now suppose that every line intersects $\mathcal{B}$ in less than x points. Using the standard equations, we shall prove that $|\mathcal{B}| \geq tq + x$ holds in this case as well, provided that x is chosen properly. We will set $x = \sqrt{tq} + 1$.

Let n_i denote the number of i-secants to $\mathcal{B}$. Recall the standard equations:

$$\sum_{i=0}^{q+1} n_i = q^2 + q + 1,$$

$$\sum_{i=0}^{q+1} in_i = |\mathcal{B}|(q+1),$$

$$\sum_{i=0}^{q+1} i(i-1)n_i = |\mathcal{B}|(|\mathcal{B}|-1).$$

Since every line intersects $\mathcal{B}$ in at least t and in at most x points, we have

$$0 \leq \sum_{i=1}^{q+1}(i-t)(x-i)n_i = -\sum_{i=1}^{q+1} i(i-1)n_i + \sum_{i=1}^{q+1}(x+t-1)in_i - \sum_{i=1}^{q+1} txn_i,$$

which combined with the standard equations gives the following quadratic inequality:

$$|\mathcal{B}|^2 - (tq + x + t + (x-1)q)\,|\mathcal{B}| + tx(q^2+q+1) \leq 0.$$

Thus $|\mathcal{B}|$ is at least as large as the smaller root of the quadratic polynomial (in the variable $|\mathcal{B}|$) on the left-hand side. Hence it is enough to prove that substituting $|\mathcal{B}| = tq + x$ in the polynomial we get a non-negative value and that $tq + x$ is not larger than the larger root. The mean of the roots, $(tq + x + t + (x-1)q)/2$, is larger than $tq + x$ iff $x \geq t + q/(q-1)$, which holds for $x = \sqrt{tq} + 1$ under $1 \leq t \leq q - 2$. (Let us remark that $x \geq \sqrt{tq} + \frac{1}{2}$ and $t \leq q - 3$ are also satisfactory here.) Thus the second condition is satisfied. Regarding the first condition, substituting $|\mathcal{B}| = tq + x$ in the polynomial we get

$$txq - t^2q + tq^2 - x(x-1)q,$$

which is non-negative if and only if

$$x^2 - (t+1)x - t(q-t) \leq 0.$$

Using $t \leq q$, it is immediate to check that for $x = \sqrt{tq} + 1$ this inequality holds. Thus $|\mathcal{B}| \geq tq + \sqrt{tq} + 1$ is proved. □

REMARK 2.3.2. *The arguments in the proof of Theorem 2.3.1 also work with* $x = \sqrt{tq} + \frac{t}{2}\left(1 - \sqrt{\frac{t}{q}}\right) + \frac{1}{2}$*, though we need a little more detailed calculations. In this way we obtain the following: if* $\mathcal{B}$ *is a* t*-fold blocking set in* Π_q *that contains no line and* $1 \le t \le q-3$*, then*

$$|\mathcal{B}| \ge tq + \sqrt{tq} + \frac{t}{2}\left(1 - \sqrt{\frac{t}{q}}\right) + \frac{1}{2}.$$

Based on Ball's theorem, an unpublished result due to Bacsó, Héger, Szőnyi and Tuza yields a similar lower bound for the case when lines are not excluded.

THEOREM 2.3.3. *Let* $\mathcal{B}$ *be a* t*-fold blocking set in an arbitrary projective plane of order* q*,* $2 \le t \le q-3$*. Then*

$$|\mathcal{B}| \ge tq + \sqrt{(t-1)q} - t + 3.$$

Proof. If $\mathcal{B}$ contains no line, then we may apply Theorem 2.3.1. If $\mathcal{B}$ contains exactly one line, then by deleting $q-t+2$ arbitrary points from it we obtain a $(t-1)$-fold blocking set that contains no line. Thus by Theorem 2.3.1, $|\mathcal{B}| \ge (t-1)q + \sqrt{(t-1)q} + 1 + q - t + 2 = tq + \sqrt{(t-1)q} - t + 3$. If $\mathcal{B}$ contains at least two lines, choose two of them. These intersect in a point P. Counting the number of points of $\mathcal{B}$ on the lines through P we get that $|\mathcal{B}| \ge 1 + 2q + (t-1)(q-1) = (t+1)q - t + 2 \ge tq + \sqrt{(t-1)q} - t + 3$. □

REMARK 2.3.4. *By Remark 2.3.2, we may obtain a somewhat better constant term in Theorem 2.3.3, namely* $|\mathcal{B}| \ge tq + \sqrt{(t-1)q} - t + \frac{5}{2} + \frac{t-1}{2}\left(1 - \sqrt{\frac{t-1}{q}}\right)$.

2.4 Remarks

Surprisingly enough, there is a shortage of constructions for multiple blocking sets in $\mathrm{PG}(2,q)$ if q is not a square. It seems that the only (rather natural) idea to construct small t-fold blocking sets for general t so far is to find and unite t disjoint blocking sets. One may ask whether every small enough t-fold blocking set in $\mathrm{PG}(2,q)$ is the union of t disjoint blocking sets, provided that t is small enough (cf. the linearity conjecture for multiple blocking sets [69]); however, this question seems quite hard. An affirmative answer for $t=2$ would improve some of the results we present later.

Chapter 3

On constructions of (k,g)-graphs

This chapter is based on the articles [D], [E], and [C]. The respective part of [C] is an attempt to give a general background of and to unify the constructions and concepts presented formerly in the topic; here we rely on this point of view.

3.1 Introduction to (k,g)-graphs

Definition 3.1.1. *A* (k,g)-graph *is a k-regular graph of girth g. The least number of vertices a (k,g)-graph may have is denoted by $c(k,g)$. A* (k,g)-cage *is a (k,g)-graph on $c(k,g)$ vertices.*

The study of cages began in the mid-1900s with the papers of Tutte [73] and Kárteszi [51]. The cases $k = 2$, $g = 3$, and $g = 4$ are trivial, the corresponding cages are the cycles, complete graphs, and the regular complete bipartite graphs, respectively. It was proved by Erdős and Sachs [35] that (k,g)-graphs exist for all $k \geq 2$ and $g \geq 3$, thus $c(k,g)$ is defined for such parameters. Determining $c(k,g)$ is challenging and extremely hard in general; for an overview on the topic, see the surveys [36] and [76]. There is a simple and well-known lower bound on $c(k,g)$. Throughout this chapter we use the following notation. For a vertex v, let $N^i(v) = \{u \in V : d(v,u) = i\}$, that is, the set of the i^{th} neighbors of v. In particular, $N^0(v) = \{v\}$ and $N^1(v) = N(v)$. If $i < 0$, let $N^i(v) = \emptyset$.

Result 3.1.2 (Moore bound).

$$c(k,g) \geq c_0(k,g) = \begin{cases} 1 + \displaystyle\sum_{i=0}^{(g-3)/2} k(k-1)^i & \textit{if } g \textit{ is odd,} \\ 2\displaystyle\sum_{i=0}^{(g-2)/2} (k-1)^i & \textit{if } g \textit{ is even.} \end{cases}$$

Proof. Let G be a (k, g)-graph. If $g = 2n + 1$ is odd, let v be an arbitrary vertex of G. As $g(G) = 2n + 1$, for all $i = 1, \ldots, n$, the set $N^i(v)$ consists of $k(k-1)^i$ pairwise distinct vertices, which yields the stated lower bound. If $g = 2n$ is even, let uv be an arbitrary edge of G. Similarly, the sets $A_i = N^i(u) \setminus N^{i-1}(v)$ and $B_i = N^i(v) \setminus N^{i-1}(u)$, $0 \leq i \leq n-1$, are pairwise disjoint of size $(k-1)^i$. $\square$

This bound was established by Tutte [73], Kárteszi [51], and Erdős and Sachs [35]. The name Moore bound originates from the same numerical bound regarding the degree/diameter problem attributed to E. F. Moore (cf. [47]).

DEFINITION 3.1.3. *A (k, g)-graph on $c_0(k, g)$ vertices is called a* Moore graph *or a* Moore cage.

By definition, Moore cages of girth $g = 2n$ and degree k and generalized n-gons of order $(k-1, k-1)$ are the same. Excluding the trivial cases, Moore cages are rare objects. They may exist only if $g = 5, 6, 8, 12$. This result is due to Damerell [31], Bannai and Ito [17] and Feit and Higman [37]. Furthermore, the celebrated Hoffman–Singleton theorem [47] says that a Moore cage of girth $g = 5$ may only have degree $k = 3, 7, 57$. In the cases $g = 6$, 8, and 12, Moore cages exist whenever the degree k is subsequent to a power of a prime. The famous and widely open prime power conjecture claims that every Moore cage of girth 6, 8 or 12 has such degree. (In other words, the conjecture says that a GP of order (q, q) exists iff q is a prime power.) For more results and interesting open problems in the topic, the reader is once again directed to the excellent surveys [36] and [76].

It is worth mentioning that in the cases $g = 6$, 8, and 12, the only known cage that is not a Moore graph is the unique $(7, 6)$-cage on 90 vertices, which is the incidence graph of an elliptic semiplane discovered by Baker [9]. Thus lower bounds and constructions are both welcome; we are focusing on the latter. Please note that although several techniques have been developed to construct small (k, g)-graphs, the recent work only treats one specific idea.

The next, fundamental result is often referred to as the girth monotonicity of the order of cages.

RESULT 3.1.4 (Erdős–Sachs [35]). *Let $k \geq 2$, $g \geq 3$. Then $c(k, g) < c(k, g + 1)$.*

Recall that a t-fold perfect dominating set (t-PDS) is a proper vertex-set in a graph such that any vertex not belonging to it has exactly t neighbors in it. Let $G = (V; E)$ be a k-regular graph, and let $W \subsetneq V$. It is clear that the subgraph G' of G induced by $V \setminus W$ is $(k-t)$-regular if and only if W is a t-PDS of G. This operation never decreases the girth, though $g(G') > g(G)$ may occur. Result 3.1.4 shows that this idea can be used to give an upper bound on $c(k-t,g)$. Clearly, for a fixed t, the larger t-PDS we find the better bound we obtain.

Starting from a projective plane of order q, Brown ([25], 1967) constructed $(k,6)$-graphs for arbitrary $4 \leq k \leq q$ by deleting some properly chosen points and lines from the plane, that is, by removing the vertices of a $(q+1-k)$-PDS from the incidence graph of the plane. Although Brown himself gave only one specific construction without any general terminology, the basic idea of deleting a t-PDS from a cage seems to appear first in his paper [25]. Thus we refer to this construction method as Brown's method. Our aim in this chapter is not only to construct small (k,g)-graphs by applying Brown's method for GPs, but to understand its limitations as well.

In [D], t-good structures were introduced to investigate the induced regular subgraphs of generalized polygons. In [1], the notion of perfect dominating sets appears in the context of constructing small $(k,8)$-graphs. In fact, t-good structures and t-PDSs are the same. Since (perfect) dominating sets have a large literature (see [45]), we decided to use the latter terminology.

However, one may look for non-induced regular subgraphs of a generalized polygon; that is, we are allowed to delete vertices and edges as well to obtain a regular graph from the incidence graph of the GP. There are constructions that prove this idea useful as we will see in Section 3.6.

3.2 Perfect t-fold dominating sets in generalized polygons

In this section we give some definitions, notation and constructions that work for all generalized polygons. In case of generalized polygons (or more generally, bipartite graphs), we consider a t-PDS as a pair of vertex-sets $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ corresponding to the vertex classes of the graph, where $\mathcal{P}_0 \cup \mathcal{L}_0$ is a t-PDS.

Notation. *If $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ is a fixed t-PDS, a line $\ell \in \mathcal{L}_0$ (a point $P \in \mathcal{P}_0$) will be called also a $\mathcal{T}$-line (a $\mathcal{T}$-point).*

Remark 3.2.1. *In [D] and [E], the term "t-good structure" is used instead of "t-PDS".*

We continue with a trivial observation.

PROPOSITION 3.2.2. *Let $G = (\mathcal{P}, \mathcal{L})$ be a generalized polygon of order q, and let $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$, $\mathcal{P}_0 \subset \mathcal{P}$, $\mathcal{L}_0 \subset \mathcal{L}$, be a t-PDS in G, $t < k$. Then $|\mathcal{P}_0| = |\mathcal{L}_0|$.*

Proof. As G and the subgraph of G induced by $(\mathcal{P} \setminus \mathcal{P}_0) \cup (\mathcal{L} \setminus \mathcal{L}_0)$ are regular bipartite graphs, we have $|\mathcal{P}| = |\mathcal{L}|$ and $|\mathcal{P}| - |\mathcal{P}_0| = |\mathcal{L}| - |\mathcal{L}_0|$. $\square$

Note that the above argument works for arbitrary regular bipartite graphs, not only GPs.

DEFINITION 3.2.3. *Let $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ be a t-PDS in a generalized polygon. We define the* size of $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ *as $|\mathcal{T}| := |\mathcal{P}_0| = |\mathcal{L}_0|$ (instead of the number $|\mathcal{P}_0| + |\mathcal{L}_0| = 2\,|\mathcal{P}_0|$ of vertices in it).*

The common combinatorial properties of generalized polygons allow us to give a general construction of t-PDSs in them. We show a purely combinatorial idea. Recall that in a graph $G = (V, E)$, $d(x, y)$ denotes the distance of x and y, and $B^r(x) = \{y \in V : d(x, y) \leq r\}$ is the ball of center x and radius r. The upcoming, general construction can be found in [C].

The neighboring balls construction.

Let $G = (\mathcal{P}, \mathcal{L})$ be the incidence graph of a generalized n-gon of order q. Let $\mathcal{L}^* = \{\ell_1, \ldots, \ell_t\}$ and $\mathcal{P}^* = \{P_1, \ldots, P_t\}$ be a collection of distinct lines and points such that $\forall 1 \leq i < j \leq t$ the following hold:

(i) $d(\ell_i, \ell_j) = 2$ (the lines are pairwise intersecting);

(ii) the unique point at distance one from ℓ_i and ℓ_j (their intersection point) is an element of $\mathcal{P}^*$;

(i') $d(P_i, P_j) = 2$ (the points are pairwise collinear);

(ii') the unique line at distance one from P_i and P_j (the line joining them) is an element of $\mathcal{L}^*$.

We call such a pair $(\mathcal{P}^*, \mathcal{L}^*)$ a *proper center-set*. Let $\mathcal{B}_{\mathcal{P}^*,\mathcal{L}^*} = (\mathcal{P}_0, \mathcal{L}_0)$ be the collection of points and lines that are at distance at most $n-2$ from some element of $\mathcal{P}^*$ or $\mathcal{L}^*$; that is, $\mathcal{P}_0 \cup \mathcal{L}_0 = \bigcup_{i=1}^{t}\{B^{n-2}(P_i)\} \cup \bigcup_{i=1}^{t}\{B^{n-2}(\ell_i)\}$.

PROPOSITION 3.2.4. *$\mathcal{B}_{\mathcal{P}^*,\mathcal{L}^*}$ is a t-PDS in G.*

Proof. We may assume that n is even (the other case is analogous). Let $Q \in \mathcal{P} \setminus \mathcal{P}_0$. Then for every $1 \le i \le t$ we have $d(Q, \ell_i) = n-1$ and $d(Q, P_i) = n$; hence there is a unique a line e_i such that $d(Q, e_i) = 1$ and $d(e_i, \ell_i) = n-2$. Thus $e_1, \dots, e_t$ are precisely those lines of $\mathcal{L}_0$ that are incident with Q. We show that these lines are pairwise distinct. Suppose to the contrary that $e_i = e_j = e$ for some $i \neq j$. Let $P \in \mathcal{P}^*$ be the point incident with both ℓ_i and ℓ_j. Then $d(Q, P) = n$, and $d(P, e) = n-1$. Consequently, there are two distinct paths of length $n-1$ from P to e, one through ℓ_i and another one through ℓ_j, a contradiction. Thus exactly t neighbors of a point Q are in $\mathcal{T}$. The same (dual) arguments hold for lines. □

We call $\mathcal{B}_{\mathcal{P}^*,\mathcal{L}^*}$ a neighboring balls union with center $(\mathcal{P}^*, \mathcal{L}^*)$. This immediately yields two specific constructions, the first of which is essentially the same as the one in the proof of Theorem 1 in [4]. In Section 3.5, we show the connections among the constructions appearing in [2, 4, 25, 56, C, D].

Construction 3.2.1: the basic t-PDS [D]. Let $\mathcal{P}^* = \{P_1, P_2, \dots, P_t\}$ be t arbitrary points on a line ℓ_1, and let $\mathcal{L}^* = \{\ell_1, \ell_2, \dots, \ell_t\}$ be t arbitrary lines through P_1 in a generalized n-gon G of order q. Then $\mathcal{B}_{\mathcal{P}^*,\mathcal{L}^*}$ is a t-PDS of size $tq^{n-2} + q^{n-3} + \ldots + q + 1$.

Proof. It is straightforward that $(\mathcal{P}^*, \mathcal{L}^*)$ is a proper center set, thus $\mathcal{B}_{\mathcal{P}^*,\mathcal{L}^*} = (\mathcal{P}_0, \mathcal{L}_0)$ is a t-PDS. Let $\mathcal{T} = \mathcal{P}_0 \cup \mathcal{L}_0$, and consider the sets $A_i = N^i(P_1) \setminus N^{i-1}(\ell_1)$ and $B_i = N^i(\ell_1) \setminus N^{i-1}(P_1)$, $0 \le i \le n-1$, which partition the vertex-set of G as seen in the proof of Result 3.1.2. Then $\bigcup_{i=0}^{n-2} A_i \subset B^{n-2}(P_1) \subset \mathcal{T}$, and $A_{n-1} \cap \mathcal{T} = A_{n-1} \cap \left(\bigcup_{i=2}^{t} B^{n-2}(\ell_i)\right)$. Thus $|\mathcal{T} \cap \left(\cup_{i=0}^{n-1} A_i\right)| = 1 + q + \ldots + q^{n-2} + (t-1)q^{n-2}$. Analogously, $|\mathcal{T} \cap \left(\cup_{i=0}^{n-1} B_i\right)| = 1 + q + \ldots + q^{n-3} + tq^{n-2}$. □

The above construction may be regarded as a generalization of Brown's construction [25], which starts from a projective plane. The next construction improves on the size for $t = 1$ by q^{n-3}. If we start from $\mathrm{PG}(2, q)$, we obtain basically the same construction that appears in [2].

Construction 3.2.2: the antiflag PDS [D]. Let (P, ℓ) be an arbitrary antiflag in a generalized n-gon G of order q ($n \in \{3, 4, 6\}$), and let $\mathcal{P}^* = \{P\}$, $\mathcal{L}^* = \{\ell\}$. Then $\mathcal{B}_{\mathcal{P}^*,\mathcal{L}^*}$ is a 1-PDS of size $\sum_{i=0}^{n-2} q^i + q^{n-3}$.

Proof. It is trivial that $(\mathcal{P}^*, \mathcal{L}^*)$ is a proper center set, thus $\mathcal{B}_{\mathcal{P}^*,\mathcal{L}^*} = (\mathcal{P}_0, \mathcal{L}_0) = \mathcal{T}$ is a 1-PDS. Suppose that $d(P, \ell) = d$. Let e a line in $B^1(P) \cap B^{d-1}(\ell)$. Note that if n is even, then $d \le n-1$, so e is unique. Consider the partition $\{A_i, B_i\}_{i=0}^{n-1}$

of G as in the proof of Result 3.1.2 with $u = P$ and $v = e$. Recall that any vertex $x \in A_i$ (B_i), $0 \leq i \leq n-1$, has q neighbors in A_{i+1} (B_{i+1}) and one in A_{i-1} (B_{i-1}), where A_n and A_{-1} (B_n and B_{-1}) are replaced by B_{n-1} and B_0 (A_{n-1} and A_0), respectively. By Proposition 3.2.2, it is enough to determine $|\mathcal{P}_0|$. Note that $\mathcal{P}_0 \cap A_i = \emptyset$ if $0 \leq i \leq n-1$ is odd, and $\mathcal{P}_0 \cap B_i = \emptyset$ if $0 \leq i \leq n-1$ is even. If $n = 3$, then $d(P, \ell) = 3$, and $B^1(P) \cap \mathcal{P}_0$ and $B^1(\ell) \cap \mathcal{P}_0$ are disjoint sets of size 1 and $q+1$, respectively, hence $|\mathcal{P}_0| = q+2$ as indicated. Now suppose that $n \in \{4, 6\}$. Then $B^{n-2}(P) \cap \mathcal{P}_0 = \left(\bigcup_{i=0}^{n/2-1} A_{2i}\right) \cup \left(\bigcup_{i=0}^{n/2-2} B_{2i+1}\right)$ contains $(q^{n-1}-1)/(q-1)$ points, so we only have to deal with $\mathcal{P}_0 \cap B_{n-1} = B^{n-2}(\ell) \cap B_{n-1}$. If $d(P, \ell) = 3$ (that is, $\ell \in B_2$; this must be the case if $n = 4$), then it is easy to see that $B_{n-1} \cap \mathcal{P}_0 = B^{n-3}(\ell) \cap \mathcal{P}_0$ has precisely q^{n-3} points, hence the assertion follows. If $d(P, \ell) = 5$ (that is, $\ell \in B_4$ and $n = 6$), then the points of $B_5 \cap \mathcal{P}_0$ can be reached from ℓ via a path of length three, $\ell - x_1 - x_2 - x_3$, where either $x_1 \in B_3$, $x_2 \in B_4$, and $x_3 \in B_5$, or $x_1 \in B_5$, $x_2 \in A_5$, $x_3 \in B_5$. We can reach $1 \cdot q \cdot q^2$ vertices in the first way (this is clear), and $q \cdot q \cdot (q-1)$ new vertices in the second way, as all vertex in A_5 has $q-1$ neighbors in B_5 which are not adjacent to ℓ (those have been found already). These two groups are disjoint as the girth of G is more than six, thus we have found q^3 points. $\square$

Note that in the neighboring balls construction, if we allow $\mathcal{P}^*$ and $\mathcal{L}^*$ to have different sizes, s and t, respectively, and define $\mathcal{T}$ the same way, then the same arguments show that after deleting $\mathcal{T}$, every non-deleted point has degree $q+1-s$ or $q+1-t$, and every non-deleted line has degree $q+1-t$ or $q+1-s$, depending on n being odd or even, respectively. More generally, one may define (s,t)-PDSs in order to obtain biregular graphs. Although biregular cages are also of interest, we will restrict the usage of (s,t)-PDSs to give a better overview of perfect dominating sets in generalized quadrangles.

DEFINITION 3.2.5. *Let $(\mathcal{P}, \mathcal{L})$ be a GP of order q. A pair of a proper point-set and a proper line-set $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ is a* perfect (s,t)-dominating set *if every point outside $\mathcal{P}_0$ is covered by s lines of $\mathcal{L}_0$, and every line outside $\mathcal{L}_0$ intersects $\mathcal{P}_0$ in t points. The* size *of an (s,t)-PDS $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ is the pair $(|\mathcal{P}_0|, |\mathcal{L}_0|)$.*

By definition, $\mathcal{T}$ is a t-PDS if and only if it is a (t,t)-PDS.

DEFINITION 3.2.6. *Let $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ be an (s,t)-PDS. A point P (a line ℓ) is* $\mathcal{T}$-complete, *if $P \in \mathcal{P}_0$ and $[P] \subset \mathcal{L}_0$ ($\ell \in \mathcal{L}_0$ and $[\ell] \subset \mathcal{P}_0$).*

Proposition 3.2.7. *Let $\mathcal{T}_i = (\mathcal{P}_i, \mathcal{L}_i)$ be an (s_i, t_i)-PDS, $i = 1, 2$. Then $\mathcal{T} = (\mathcal{P}_1 \cup \mathcal{P}_2, \mathcal{L}_1 \cup \mathcal{L}_2)$ is an $(s_1 + s_2, t_1 + t_2)$-PDS if and only if every point in $\mathcal{P}_1 \cap \mathcal{P}_2$ and every line in $\mathcal{L}_1 \cap \mathcal{L}_2$ is $\mathcal{T}$-complete.*

Proof. Let $\mathcal{P}_0 = \mathcal{P}_1 \cup \mathcal{P}_2$, $\mathcal{L}_0 = \mathcal{L}_1 \cup \mathcal{L}_2$. Then $[P] \cap \mathcal{L}_0 = s_1 + s_2$ for all $P \notin \mathcal{P}_0$ if and only if $[P] \cap \mathcal{L}_1 \cap \mathcal{L}_2 = \emptyset$ for all $P \notin \mathcal{P}_0$, which holds if and only if every line of $\mathcal{L}_1 \cap \mathcal{L}_2$ is $\mathcal{T}$-complete. By duality, we are ready. □

Corollary 3.2.8. *The union of a $(0, t)$-PDS and an $(s, 0)$-PDS is an (s, t)-PDS.*

Proof. The lines of a $(0, t)$-PDS $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ must be $\mathcal{T}$-complete, otherwise there would be a point $P \notin \mathcal{P}_0$ incident with at least one line of $\mathcal{L}_0$. Similarly, the points of an $(s, 0)$-PDS are also complete, hence the assertion follows by Proposition 3.2.7. □

3.3 Perfect t-fold dominating sets in projective planes

This section is based on [D, E]. Throughout this section $\Pi_q = (\mathcal{P}, \mathcal{L})$ denotes a finite projective plane of order q. Recall that $|\mathcal{P}| = |\mathcal{L}| = q^2 + q + 1$. We recall and rephrase the definition of t-PDSs for projective planes.

Definition 3.3.1. *Let $(\mathcal{P}, \mathcal{L})$ be a finite projective plane, $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$, $\mathcal{P}_0 \subsetneq \mathcal{P}$, $\mathcal{L}_0 \subsetneq \mathcal{L}$. $\mathcal{T}$ is a* perfect t-fold dominating set *iff*

- *$\forall P \notin \mathcal{P}_0$ there are exactly t lines in $\mathcal{L}_0$ through P,*
- *$\forall \ell \notin \mathcal{L}_0$ there are exactly t points in $\mathcal{P}_0$ on ℓ.*

3.3.1 Constructions

The first two constructions are also related to the work of other authors. These relations are discussed in Section 3.5.

Construction 3.3.1: complete subplanes [D, E]. Let $(\mathcal{P}^*, \mathcal{L}^*)$ be a (possibly degenerate) subplane, $\mathcal{P}^* = \{P_1, \ldots, P_t\}$, $\mathcal{L}^* = \{\ell_1, \ldots, \ell_t\}$. Let $\mathcal{P}_0 = \mathcal{P}^* \bigcup \cup_{i=1}^{t} [\ell_i]$, $\mathcal{L}_0 = \mathcal{L}^* \bigcup \cup_{i=1}^{t} [P_i]$. Then $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ is a t-PDS. The size of $\mathcal{T}$ is $tq + 1$, $t(q-1) + 3$, $t(q - t_1 + 1)$ according to whether the underlying subplane is degenerate of type π_1 or π_2, or it is nondegenerate of order t_1, where $t = t_1^2 + t_1 + 1$, respectively.

Proof. Let $P \notin \mathcal{P}_0$. Then $P \notin l_i$ $(i = 1, \ldots, t)$, and the lines $P \cap P_i$, $i = 1, \ldots, t$ are pairwise distinct elements of $\mathcal{L}_0$ as the lines connecting any two of the P_is are in $\mathcal{L}^*$ as $(\mathcal{P}^*, \mathcal{L}^*)$ is a subplane. Hence the number of $\mathcal{T}$-lines through P is t. The dual arguments for lines finish the proof. Calculating the sizes is easy. □

The above construction is a rephrasal of the neighboring balls construction for projective planes; a proper center set is simply a (possibly degenerate) subplane. Constructions 3.2.1 and 3.2.2 correspond to a complete degenerate subplane of type π_1 and π_2 (the latter one consisting of a single antiflag), respectively. Note that for $t = 2$, both degenerate subplanes yield the same 2-PDS.

Construction 3.3.2: disjoint Baer subplanes [D]. Let $B_i = (\mathcal{P}_i, \mathcal{L}_i)$, $i = 1, \ldots, t$, be t mutually disjoint Baer subplanes. Let $\mathcal{P}_0 = \cup_{i=1}^t \mathcal{P}_i$, $\mathcal{L}_0 = \cup_{i=1}^t \mathcal{L}_i$. Then $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ is a t-PDS of size $t(q + \sqrt{q} + 1)$.

Proof. Every line intersects a Baer subplane in one or $\sqrt{q} + 1$ points. Respective lines are called tangents and long secants. If P is a point not in a Baer subplane, then there are q tangent lines and exactly one long secant through it. Given two disjoint Baer subplanes, there is no line intersecting both in $\sqrt{q} + 1$ points [24]. Thus $\mathcal{L}_0$ covers every point not in $\mathcal{P}_0$ exactly t-times. Similarly, every line not in $\mathcal{L}_0$ intersects each $\mathcal{P}_i$ $(i = 1, \ldots, t)$ in exactly one point, hence $\mathcal{P}_0$ intersects these lines in precisely t points. □

Construction 3.3.3: unital. Let $\mathcal{U}$ be a unital in Π_q. Let $\mathcal{P}_0 = \mathcal{U}$, and let $\mathcal{L}_0$ be the set of tangent lines to $\mathcal{U}$. Then $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ is a $(\sqrt{q} + 1)$-PDS of size $q\sqrt{q} + 1$.

Proof. A line not in $\mathcal{L}_0$ intersects $\mathcal{U}$ in $\sqrt{q} + 1$ points by definition. Through a point not in $\mathcal{U}$ there are exactly $\sqrt{q} + 1$ tangents to $\mathcal{U}$. □

Construction 3.3.4: maximal $\sqrt{q}$-arc. Let $\mathcal{K}$ be an $(n, \sqrt{q})$-arc in Π_q of size $n = \sqrt{q}\left(q - \sqrt{q} + 1\right)$. Let $\mathcal{P}_0 = \mathcal{K}$, and let $\mathcal{L}_0$ be the set of skew lines to $\mathcal{K}$. Then $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ is a $\sqrt{q}$-PDS of size n.

Proof. Every line intersects $\mathcal{K}$ in zero or $\sqrt{q}$ points. Lines not in $\mathcal{L}_0$ intersect $\mathcal{P}_0 = \mathcal{K}$ in $\sqrt{q}$ points by definition. Through a point not in $\mathcal{P}_0$ there are exactly $\sqrt{q}$ skew lines and $q - \sqrt{q} + 1$ $\sqrt{q}$-secants to $\mathcal{P}_0$. □

Construction 3.3.5: inner part of an oval. Let $\mathcal{O}$ be an oval of Π_q, q odd. Let $\mathcal{P}_0 = \mathcal{O} \cup \mathrm{Inn}(\mathcal{O})$, $\mathcal{L}_0 = \mathrm{Tan}(\mathcal{O}) \cup \mathrm{Skw}(\mathcal{O})$. Then $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ is a $(q+1)/2$-PDS of size $q(q + 1)/2$.

Proof. Recall that on a two-secant line there are $(q-1)/2$ outer points of $\mathcal{O}$, while on an outer point of $\mathcal{O}$ there are $(q-1)/2$ two-secant lines. The number of outer points is $q(q+1)/2$. $\square$

Construction 3.3.6: outer part of an oval. Let $\mathcal{O}$ be an oval of Π_q, q odd. Let $\mathcal{P}_0 = \mathcal{O} \cup \mathrm{Out}(\mathcal{O})$, $\mathcal{L}_0 = \mathrm{Tan}(\mathcal{O}) \cup \mathrm{Sec}(\mathcal{O})$. Then $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ is a $(q-1)/2$-PDS of size $q(q-1)/2$.

Proof. Recall that on a skew line there are $(q+1)/2$ inner points of $\mathcal{O}$, while on an inner point of $\mathcal{O}$ there are $(q+1)/2$ skew lines. The number of inner points is $q(q-1)/2$. $\square$

Construction 3.3.7: half-line. Let $\ell = \{P_0, \dots, P_q\}$ be a line, and $P \notin \ell$ an arbitrary point of Π_q, q odd. Let $\mathcal{P}_0 = [\ell] \bigcup \cup_{i=0}^{\lfloor q/2 \rfloor} [P \cap P_i]$, and let $\mathcal{L}_0 = [P] \bigcup \cup_{i=\lceil q/2 \rceil}^{q} [P_i]$. Then $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ is a $(q+1)/2$-PDS of size $(q+1)^2/2 + 1$.

Proof. A line $e \notin \mathcal{L}_0$ is not incident with P or P_i, $i = \lceil q/2 \rceil, \dots, q$ and thus the $\mathcal{T}$-points on e are exactly its intersections with the lines $P \cap P_i$, $0 \leq i \leq \lfloor q/2 \rfloor$. $\square$

In the above list there are only two constructions that provide us t-PDSs for arbitrary values of t, namely Constructions 3.3.1 and 3.3.2, which will be referred to as complete (degenerate) subplanes and disjoint Baer subplanes in the sequel, respectively. Furthermore, all other constructions yield t-PDSs with $t \geq \sqrt{q}$. In what follows, our aim is to study t-PDSs in finite projective planes, and, assuming that t is small enough, to characterize all of them in $\mathrm{PG}(2,q)$.

For a point P, $[P]$ covers all but one points exactly once; for t points $P_1, \dots, P_t$, $\cup_{i=1}^{t} [P_i]$ covers a lot of points exactly t times, so it is natural to ask how one can construct a t-PDS by putting t points and lines completely into it. The sharpness of the following result is shown by Construction 3.3.7.

PROPOSITION 3.3.2 ([E]). *Let $t < (q+1)/2$, $\mathcal{P}^* = \{P_1, \dots, P_t\}$ and $\mathcal{L}^* = \{\ell_1, \dots, \ell_t\}$, $\mathcal{P}_0 = \mathcal{P}^* \bigcup \cup_{i=1}^{t} [\ell_i]$, $\mathcal{L}_0 = \mathcal{L}^* \bigcup \cup_{i=1}^{t} [P_i]$. Then $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ is a t-PDS in Π_q if and only if $(\mathcal{P}^*, \mathcal{L}^*)$ is a (possibly degenerate) subplane.*

Proof. As the if part was proved in Construction 3.3.1, we only discuss the only if part. Take a line connecting two (or more) of the P_is, and suppose that there is a point P on it that is not in $\mathcal{P}_0$. Then some of the $\mathcal{T}$-lines $P \cap P_i$ coincide, and as P is not incident with any $\ell \in \mathcal{L}^*$, there are less than t $\mathcal{T}$-lines through P, a contradiction. Hence lines connecting the points of $\mathcal{P}^*$ must be $\mathcal{T}$-complete. A line $\ell \notin \mathcal{L}^*$ may intersect $\mathcal{P}^*$ in at most t points and may contain t further

$\mathcal{T}$-points on the ℓ_is. As $2t < q+1$, we get that there are no $\mathcal{T}$-complete lines outside $\mathcal{L}^*$. Together with the dual of this argument, we see that $(\mathcal{P}^*, \mathcal{L}^*)$ is a subplane. □

3.3.2 General results

PROPOSITION 3.3.3 ([D]). *Let $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ be a t-PDS in Π_q, $t \le q$. Then $|\mathcal{T}| \ge t(q+1-t)$. In case of equality $t = \sqrt{q}$ and $\mathcal{P}_0$ is a maximal $(\sqrt{q}, n)$-arc.*

Proof. Take a line $e \notin \mathcal{L}_0$. Then there are exactly $q+1-t$ points not in $\mathcal{P}_0$ on e, each being incident with exactly t $\mathcal{T}$-lines. Thus we see at least $t(q+1-t)$ $\mathcal{T}$-lines.

Now suppose that equality holds. Take any line $\ell \notin \mathcal{L}_0$. Then the former argument shows that a point $P \in \ell$ is covered either zero or t times by $\mathcal{L}_0$ depending on P being in $\mathcal{P}_0$ or not, respectively. Thus $t \le q$ implies that points not in $\mathcal{P}_0$ are all covered exactly t times by $\mathcal{L}_0$. Also, for any point $P \in \mathcal{P}_0$, $|[P] \cap \mathcal{L}_0|$ is either zero or $q+1$. Should there be a point $P \in \mathcal{P}_0$ with $[P] \subset \mathcal{L}_0$, all points of $\mathcal{P}_0$ would be covered at least once, hence $q+1$ times by $\mathcal{L}_0$, which is clearly impossible. Hence the points of $\mathcal{P}_0$ are not covered by $\mathcal{L}_0$. Therefore $\mathcal{L}_0$ is a maximal dual t-arc, and dually, $\mathcal{P}_0$ is a maximal t-arc. Counting the points of $\mathcal{P}_0$ through the lines of $[P]$, $P \in \mathcal{P}_0$, we get that $1+(q+1)(t-1) = |\mathcal{P}_0| = t(q+1-t)$, whence $t = \sqrt{q}$ follows. □

PROPOSITION 3.3.4. *Let $G = (V; E)$ be a (k, g)-graph on n vertices, and let $S \subset V$ be a t-PDS of G. Then $|S| \le n - c_0(k-t, g)$.*

Proof. The subgraph of G induced by the vertices of $V \setminus S$ is $(k-t)$-regular of girth at least g, hence by the Moore bound and the girth monotonicity (Results 3.1.2 and 3.1.4) $n - |S| \ge c_0(k, g)$ follows. □

The next theorem is am important upper bound which shows that the disjoint Baer subplanes construction is optimal if t is not too large.

THEOREM 3.3.5 ([D]). *Let $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ be a t-PDS in $\Pi_q = (\mathcal{P}, \mathcal{L})$, and suppose $t \le 2\sqrt{q}$. Then $|\mathcal{T}| \le t(q+\sqrt{q}+1)$. Moreover, in case of equality every line intersects $\mathcal{P}_0$ in t or $\sqrt{q}+t$ points.*

Proof. Let

$$n_i^0 = |\{\ell \in \mathcal{L}_0 \colon |\ell \cap \mathcal{P}_0| = i\}|,$$
$$n_i^1 = |\{\ell \notin \mathcal{L}_0 \colon |\ell \cap \mathcal{P}_0| = i\}|.$$

Then the total number n_i of i-secants to $\mathcal{P}_0$ is $n_i = n_i^0 + n_i^1$. By the definition of t-PDSs,

$$n_i^1 = \begin{cases} q^2+q+1-|\mathcal{L}_0| & \text{for } i = t, \\ 0 & \text{otherwise.} \end{cases} \qquad (*)$$

Using $(*)$, the standard equations and $|\mathcal{P}_0| = |\mathcal{L}_0|$ (Proposition 3.2.2), we obtain

$$\sum_{i=0}^{q+1} n_i^0 = |\mathcal{L}_0|\,,$$

$$\sum_{i=0}^{q+1} i n_i^0 = |\mathcal{L}_0|\,(q+1+t) - t(q^2+q+1),$$

$$\sum_{i=0}^{q+1} i(i-1)n_i^0 = |\mathcal{L}_0|^2 + |\mathcal{L}_0|\,(t^2-t-1) - t(t-1)(q^2+q+1).$$

From the three equations above we get

$$\begin{aligned} 0 \;\leq\; & \sum_{i=0}^{q+1} (i-(\sqrt{q}+t))^2 n_i^0 = \\ & \sum_{i=0}^{q+1} i(i-1)n_i^0 - \sum_{i=0}^{q+1} (2(\sqrt{q}+t)-1) i n_i^0 + \sum_{i=0}^{q+1} (\sqrt{q}+t)^2 n_i^0 = \\ & |\mathcal{L}_0|^2 + |\mathcal{L}_0| \left(t^2-t-1-(2(\sqrt{q}+t)-1)(q+1+t)+(\sqrt{q}+t)^2\right) + \\ & (q^2+q+1)\left((2t(\sqrt{q}+t)-t)-t(t-1)\right) = \\ & \left(|\mathcal{L}_0| - t(q+\sqrt{q}+1)\right)\left(|\mathcal{L}_0| - (t+2\sqrt{q})(q-\sqrt{q}+1)\right). \end{aligned}$$

Hence either $|\mathcal{L}_0| \leq t(q+\sqrt{q}+1)$ or $|\mathcal{L}_0| \geq (t+2\sqrt{q})(q-\sqrt{q}+1)$ (it is easy to check that the first root is smaller than the second one). Assuming the latter case, Corollary 3.3.4 yields $2(q^2+q+1) - c_0(q+1-t, 6) = 2t(2q-t+1) \geq 2\,|\mathcal{L}_0| \geq 2(t+2\sqrt{q})(q-\sqrt{q}+1)$, in contradiction with $t \leq 2\sqrt{q}$. Therefore $|\mathcal{L}_0| \leq t(q+\sqrt{q}+1)$ must hold. Equality yields that all lines of $\mathcal{L}_0$ intersect $\mathcal{P}_0$ in $\sqrt{q}+t$ points. □

PROPOSITION 3.3.6 ([D]). *Let $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ be a t-PDS in Π_q, and assume $t \leq \sqrt{q}$. Then $\mathcal{P}_0$ is a blocking set, unless $t = \sqrt{q}$ and $\mathcal{P}_0$ is a maximal $\sqrt{q}$-arc.*

Proof. Assume that there exists a line ℓ not meeting $\mathcal{P}_0$. Then ℓ must be in $\mathcal{L}_0$. Since any point P on ℓ is outside $\mathcal{P}_0$, the number of $\mathcal{T}$-lines different from ℓ through P has to be exactly $t-1$, therefore $|\mathcal{L}_0| = 1+(q+1)(t-1) = tq+t-q$. Compared with Proposition 3.3.3, we get $t(q+1-t) \leq tq+t-q$. If $t < \sqrt{q}$, this is not possible, hence $\mathcal{P}_0$ is a blocking set. If $t = \sqrt{q}$, then we obtain equality in Proposition 3.3.3, hence $\mathcal{P}_0$ is a maximal $\sqrt{q}$-arc. □

Now the characterization of (one-fold) perfect dominating sets quickly follows.

THEOREM 3.3.7 ([D]). *Every* PDS *of* Π_q *is one of Constructions 3.3.1 and 3.3.2 (with* $t = 1$*).*

Proof. Let $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ be a perfect dominating set. First note that by Proposition 3.3.6, $\mathcal{P}_0$ is a blocking set. Since a line not in $\mathcal{L}_0$ meets $\mathcal{P}_0$ in exactly $t = 1$ point, every line joining two points of $\mathcal{P}_0$ must be a $\mathcal{T}$-line, and dually, the intersection point of two $\mathcal{T}$-lines is in $\mathcal{P}_0$. We distinguish three cases according to the maximum number ν of points in general position in $\mathcal{P}_0$.

CASE 1: $\nu = 2$. Then $\mathcal{P}_0$ is contained in a line, but since it is a blocking set, it has to be the full line. It is easy to see that $\mathcal{T}$ is obtained from Construction 3.3.1 with a degenerate subplane of type π_1.

CASE 2: $\nu = 3$. In this case $|\mathcal{P}_0| \leq q + 2$, since it cannot contain two pairs of points on two different lines, as that would imply $\nu \geq 4$. By Result 1.5.6, $\mathcal{P}_0$ has to contain a line, thus $|\mathcal{P}_0| = q + 2$. It is easy to see that $\mathcal{T}$ is obtained from Construction 3.3.1 with a degenerate subplane of type π_2.

CASE 3: $\nu \geq 4$. Assume that $\mathcal{P}_0$ contains all the points of a line ℓ. Then by $\nu \geq 4$, there must be at least two points of $\mathcal{P}_0$ not on ℓ, but then the lines joining these two points to the points of ℓ must be $\mathcal{T}$-lines, thus $|\mathcal{L}_0| \geq 2q + 2$, contradicting the upper bound $|\mathcal{P}_0| \leq q + \sqrt{q} + 1$ of Theorem 3.3.5. Therefore $\mathcal{P}_0$ is a blocking set that does not contain a full line, hence by Result 1.5.6 and Theorem 3.3.5 it is a Baer subplane, that is, we have Construction 3.3.2. $\square$

The next result yields that a 2-PDS $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ in Π_q, $q \geq 5$, is either obtained from Construction 3.3.1, or $\mathcal{P}_0$ is a double blocking set. This is not satisfactory to give a complete description of 2-PDSs in Π_q due to the lack of our recent knowledge on double blocking sets in general finite projective planes, yet it will be useful when characterizing 2-PDSs in $\mathrm{PG}(2, q)$.

PROPOSITION 3.3.8 ([D]). *Let* $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ *be a* t*-PDS in* $\Pi_q = (\mathcal{P}, \mathcal{L})$*,* $t < \sqrt{q}$*.*

1. *If* $t = 2$*, then* $|\mathcal{P}_0| = |\mathcal{L}_0| \geq 2q + 1$ *with equality if and only if* $\mathcal{T}$ *is a complete degenerate subplane.*

2. *If* $t \geq 2$ *and* $|\mathcal{T}| \geq tq + 2$*, then* $\mathcal{P}_0$ *is a double blocking set.*

Proof. To prove the first statement, let $P \notin \mathcal{P}_0$. There are $q - 1$ lines not in $\mathcal{L}_0$ through P, each containing exactly two points of $\mathcal{P}_0$. Therefore $|\mathcal{P}_0| = |\mathcal{L}_0| =$

$2q-2+c$, where c denotes the number of $\mathcal{T}$-points on the two $\mathcal{T}$-lines through P. As $2<\sqrt{q}$, Proposition 3.3.6 yields that $\mathcal{P}_0$ is a blocking set, so we can deduce that $c \geq 2$. Hence $|\mathcal{P}_0| \geq 2q$ with equality if and only if both $\mathcal{T}$-lines through P meet $\mathcal{P}_0$ in one point. Assume $|\mathcal{P}_0| \leq 2q+1$. Then $c \leq 3$. Therefore, as one can repeat this counting from any $P \notin \mathcal{P}_0$, we see that each line $\ell \in \mathcal{L}_0$ meets $\mathcal{P}_0$ in 1, 2 or $q+1$ points. Take a point $P \in \mathcal{P}_0$. Count the points of $\mathcal{P}_0$ through the lines of P. As $|\mathcal{P}_0| > q+2$, we see that there must be at least one line ℓ intersecting $\mathcal{P}_0$ in more than two points. Hence $\ell \in \mathcal{L}_0$ and $[\ell] \subset \mathcal{P}_0$. Now as $|\mathcal{P}_0| \geq 2q > q+2$, there must be two points in $\mathcal{P}_0$, Q and R, such that neither Q nor R is on ℓ. Consequently, the line $Q \cap R$ intersects $\mathcal{P}_0$ in at least three, hence in $q+1$ points, whence $|\mathcal{P}_0| \geq 2q+1$. Since we assumed $|\mathcal{P}_0| \leq 2q+1$, we obtained that $|\mathcal{P}_0| = 2q+1$ and it is the union of the point-sets of two lines. Dually, $\mathcal{L}_0$ must be the union of the line-sets of two points. Hence by Proposition 3.3.2, $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ is a complete degenerate subplane.

Now for the second statement, assume $t \geq 2$ and $|\mathcal{L}_0| \geq tq+2$. As $t \geq 2$, we only have to check that $|\ell \cap \mathcal{P}_0| \geq 2$ for all $\ell \in \mathcal{L}_0$. Suppose to the contrary. Then, as $\mathcal{P}_0$ has already been proved to be a blocking set in Proposition 3.3.6, there exists a line $\ell \in \mathcal{L}_0$ such that $\ell \cap \mathcal{P}_0 = \{P\}$. Then counting the $\mathcal{T}$-lines through the points of ℓ, we obtain $|\mathcal{L}_0| \leq 1+q+q(t-1)$, a contradiction. □

The following observation says that a proper part of a t-PDS cannot be a t-PDS. We will use this in the next subsection.

PROPOSITION 3.3.9 ([E]). *Let* $1 \leq t \leq q/2$, $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ *and* $\mathcal{T}' = (\mathcal{P}_0', \mathcal{L}_0')$ *be two t-PDSs in* $\Pi_q = (\mathcal{P}, \mathcal{L})$. *Then* $\mathcal{P}_0 \subset \mathcal{P}_0'$ *and* $\mathcal{L}_0 \subset \mathcal{L}_0'$ *implies* $\mathcal{T} = \mathcal{T}'$.

Proof. Suppose to the contrary that $\mathcal{T} \neq \mathcal{T}'$. By duality we may assume that $\mathcal{L}_0$ is a proper subset of $\mathcal{L}_0'$. Take a line $\ell \in \mathcal{L}_0' \setminus \mathcal{L}_0$. Then ℓ contains exactly $q+1-t$ points, $P_1, \ldots, P_{q+1-t}$, that are not in $\mathcal{P}_0$. Thus these are covered exactly t times by the lines of $\mathcal{L}_0$, that is, there are $q+1-t$ lines not in $\mathcal{L}_0$ through each of the P_is ($i = 1, \ldots, q+1-t$) intersecting $\mathcal{P}_0$ in exactly t points. The set S of these lines has $(q+1-t)^2$ pairwise distinct elements, and $S \cap \mathcal{L}_0 = \emptyset$. As $\ell \in \mathcal{L}_0'$ and $\mathcal{L}_0 \subset \mathcal{L}_0'$, the P_is are covered at least $t+1$ times by $\mathcal{L}_0'$, hence they are in $\mathcal{P}_0'$, thus ℓ is completely in $\mathcal{T}'$. Therefore the lines of S intersect $\mathcal{P}_0'$ in at least $t+1$ points (by $\mathcal{P}_0 \subset \mathcal{P}_0'$), hence $S \subset \mathcal{L}_0'$. Consequently, the P_is ($i = 1, \ldots, q+1-t$) are completely in $\mathcal{T}'$. Thus a point $P \notin \ell$ is covered at least $(q+1-t)$-times by $\mathcal{L}_0'$, which is more than t as $t < (q+1)/2$. This means that every point is in $\mathcal{P}_0'$, a contradiction. □

3.3.3 Characterization in $\mathrm{PG}(2, q)$

Recall that perfect dominating sets in an arbitrary finite projective plane of order q are characterized in Theorem 3.3.7. 2-PDSs can be handled separately due to Proposition 3.3.8.

THEOREM 3.3.10 ([D]). *Let $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ be a 2-PDS in* $\mathrm{PG}(2, q)$.

1. *If $q \geq 9$, then $\mathcal{T}$ is either a complete subplane, or $|\mathcal{T}| = 2(q + \sqrt{q} + 1)$.*
2. *If $q > 256$, then $\mathcal{T}$ is either a complete subplane or the union of two disjoint Baer subplanes.*

Proof. Proposition 3.3.8 yields that if $\mathcal{T}$ is not a complete subplane, then $\mathcal{P}_0$ is a double blocking set. Result 1.5.7 claims that if $q \geq 9$, then a double blocking set in $\mathrm{PG}(2, q)$ has at least $2(q + \sqrt{q} + 1)$ points. It follows from the upper bound in Theorem 3.3.5 that equality must hold. Moreover, if $q > 256$, then by Remark 1.5.9, a double blocking set of size $2(q + \sqrt{q} + 1)$ is the union of the point-sets of two disjoint Baer subplanes. Then $\mathcal{L}_0$ is the union of the line-sets of the Baer subplanes, as a line from the union intersects $\mathcal{P}_0$ in $\sqrt{q} + 2 > 2$ points. $\square$

In the rest of this section we prove our following, main result, which describes all t-PDSs in $\mathrm{PG}(2, q)$ if t is small enough (roughly, $t \leq p$ and $t \leq \sqrt[6]{q}$).

THEOREM 3.3.11 ([E]). *Let $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ be a t-PDS in $\mathrm{PG}(2, q)$, $q = p^h$, p a prime; furthermore,*

- *for $h = 1$ and $h = 2$, let $t < p^{1/2}/2$;*
- *for $h \geq 3$, let $t < \min\{p + 1, c_p q^{1/6} - 1, q^{1/4}/2\}$, where $c_2 = c_3 = 2^{-1/3}$ and $c_p = 1$ for $p > 3$.*

Then $\mathcal{T}$ is a complete (degenerate) subplane or $\mathcal{T}$ is the union of t disjoint Baer subplanes.

Throughout this section $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ will denote a t-PDS in $\mathrm{PG}(2, q)$. We will suppose $t \geq 3$, as the cases $t = 1$ and $t = 2$ have been proved already in Theorems 3.3.7 and 3.3.10.

DEFINITION 3.3.12. *We call a line* bad *if it does not intersect $\mathcal{P}_0$ in $t \mod p$ points. Dually, we call a point* bad *if it does not have $t \mod p$ lines from $\mathcal{L}_0$ through it. A point (line) is* good *if it is not bad.*

Clearly, every line not in $\mathcal{L}_0$ is good (as it intersects $\mathcal{P}_0$ in exactly t points); in other words, the bad lines are in $\mathcal{L}_0$. However, lines of $\mathcal{L}_0$ are not necessarily bad (see Figure 3.3.3). The dual observations for points stand as well.

Note that if we supposed that $q = p$ prime, then in the above definition t mod p and exactly t would be the same (assuming $t \geq 2$).

DEFINITION 3.3.13. *Let the* index *of a point P be the number of bad lines going through it. Dually, the* index *of a line ℓ is the number of bad points on it. We denote the index of a point P or a line ℓ by* $\mathrm{ind}(P)$ *and* $\mathrm{ind}(\ell)$*, respectively. For the sake of simplicity, the index of the ideal point (m), $m \in \mathrm{GF}(q)$, will be denoted by* $\mathrm{ind}(m)$ *instead of* $\mathrm{ind}((m))$.

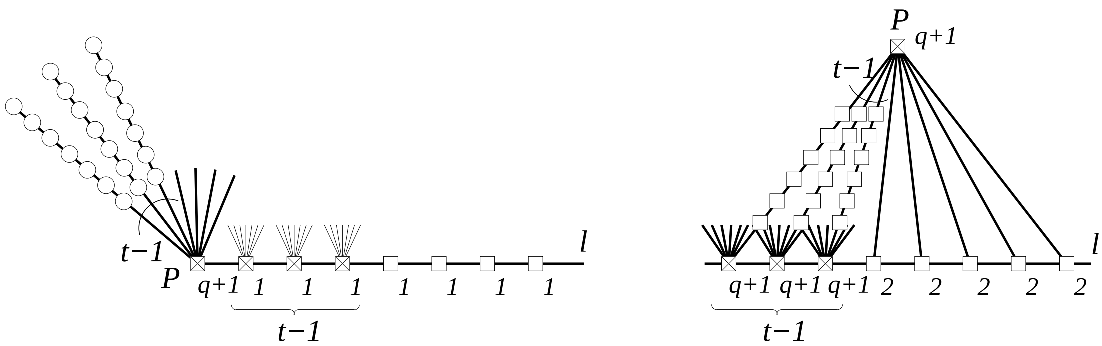

Figure 3.1: *We see the schematic pictures of two t-PDSs, a complete degenerate subplane of type π_1 and π_2, respectively. Every depicted object is in $\mathcal{T}$. Good lines are thin, bad lines are thick; good points are round, bad points are square, $\mathcal{T}$-complete points are crossed. The numbers next to the points are their indices. Note that in case of the left construction, being bad and being in $\mathcal{T}$ are not equivalent; moreover, not every $\mathcal{T}$-complete point has large index.*

Next our aim is to show that the indices of the points are either small (at most t), or large (at least $q+1-t$). First we introduce a polynomial that encodes the intersection multiplicity of $\mathcal{P}_0$ with lines. Let ℓ_∞ denote the line at infinity in an affine coordinate system. Let $\{(x_i, y_i)\}_i$ be the set of affine points of $\mathcal{T}$ (in this coordinate system), and let $\{(m_j)\}_j$ be the set of points of $\mathcal{T}$ on $\ell_\infty \setminus \{(\infty)\}$. Consider the following polynomial in $\mathrm{GF}(q)[M, B]$:

$$g(M,B) = \sum_{i=1}^{|\mathcal{P}_0 \setminus \ell_\infty|} \left(1 - (Mx_i + B - y_i)^{q-1}\right) + \sum_{(m_j) \in \mathcal{P}_0 \cap \ell_\infty} \left(1 - (M - m_j)^{q-1}\right) - t.$$

Let $m, b \in \mathrm{GF}(q)$ and let ℓ be the line defined by $Y = mX + b$. Then $g(m,b) = |\ell \cap \mathcal{P}_0| - t \pmod p$, as a term of the first or the second sum equals one if and only if the corresponding affine point (x_i, y_i) or the ideal point (m_j) is on ℓ, respectively.

PROPOSITION 3.3.14 ([E]). *Assume that ℓ_∞ is good. Then for any point $(m) \in \ell_\infty$, $m \in \mathrm{GF}(q)$, $\mathrm{ind}(m) = q - \deg\gcd\left(g(m,B), B^q - B\right)$.*

Proof. Since $b \in \mathrm{GF}(q)$ is a root of $g(m, B)$ if and only if the line $Y = mX + b$ intersects $\mathcal{P}_0$ in $t \bmod p$ points, the number of affine good lines equals the number of distinct roots of $g(m, B)$, which is precisely the degree of the greatest common divisor of $g(m, B)$ and $B^q - B$. As ℓ_∞ is good, all the bad lines are among the q affine lines passing through (m), hence the assertion follows. $\square$

As indices can be expressed in terms of the greatest common divisor of two suitable polynomials as shown above, the Szőnyi–Weiner Lemma can be applied to derive that there are no average indices.

PROPOSITION 3.3.15 ([E]). *Let k be the index of a point or a line and let $3 \leq t \leq \sqrt{q}/2$. Then either $k \leq t$ or $k \geq q + 1 - t$.*

Proof. By duality it is enough to prove the statement for the index of points. Let δ denote the total number of bad lines. As bad lines are in $\mathcal{L}_0$, Theorem 3.3.5 implies $\delta \leq |\mathcal{L}_0| \leq t(q+\sqrt{q}+1)$. Pick an arbitrary point P. If there is no good line through P, then $\mathrm{ind}(P) = q + 1$ and there is nothing to prove. Otherwise choose our coordinate system so that ℓ_∞ is a good line through P and $P = (m_0)$ is an ideal point different from (∞). Then $\delta \geq \sum_{m\in\mathrm{GF}(q)} \mathrm{ind}(m)$, as on the right-hand side we count all but the vertical bad lines exactly once. Let $u(B, M) = B^q - B$, $v(B, M) = g(M, B)$, and let $k_m = \deg\gcd(u(B, m), v(B, m))$. By Proposition 3.3.14 we have $\mathrm{ind}(m) = q - k_m$, so using the Szőnyi–Weiner Lemma we obtain

$$q \cdot \mathrm{ind}\,(m_0) - \delta \leq \sum_{m\in\mathrm{GF}(q)} \left(\mathrm{ind}\,(m_0) - \mathrm{ind}\,(m)\right) \leq \sum_{m\in\mathrm{GF}(q)} \left(k_m - k_{m_0}\right)^+ \leq$$

$$(\deg u - k_{m_0})(\deg v - k_{m_0}) = \mathrm{ind}\,(m_0)\left(\mathrm{ind}\,(m_0) - 1\right).$$

This implies

$$\mathrm{ind}(P)\left(q + 1 - \mathrm{ind}(P)\right) \leq \delta. \tag{3.1}$$

As $\delta \leq t(q + \sqrt{q} + 1)$, we get that

$$\mathrm{ind}(P)(q + 1 - \mathrm{ind}(P)) - t(q + \sqrt{q} + 1) \leq 0.$$

Since indices are integers, we only need that for $\mathrm{ind}(P) = t+1$ and $\mathrm{ind}(P) = q-t$, the above inequality does not hold. Substituting either values and using $t \leq \sqrt{q}/2$

we get $0 \geq t(q-t)-t(q+\sqrt{q}+1) = q-t(\sqrt{q}+t+2) \geq q/4-\sqrt{q}$, a contradiction if $q > 16$. As $t \geq 3$, $t \leq \sqrt{q}/2$ implies $q > 16$, hence the proof is complete. $\square$

Now we see that it $t \leq \sqrt{q}/2$, then the points and the lines can be split into two groups: the ones with small and the others with large index.

DEFINITION 3.3.16. *The index of a point or a line is called* large, *if it is at least $q+1-t$, and it is called* small, *if it is at most t.*

Note that as bad lines are in $\mathcal{L}_0$, the number of $\mathcal{T}$-lines through a point with large index is at least $q+1-t$, which is larger than t (provided that $t < (q+1)/2$), hence such points are in $\mathcal{P}_0$. Let us examine points and lines with large index.

PROPOSITION 3.3.17 ([E]). *If $3 \leq t \leq \sqrt{q}/2$, then points and lines with large index are $\mathcal{T}$-complete.*

Proof. By duality it is enough to prove the proposition for points. Suppose to the contrary that there is a point P with large index and a line $\ell \notin \mathcal{L}_0$ passing through P. Thus $|\ell \cap \mathcal{P}_0| = t$. We count the number of $\mathcal{T}$-lines through the points of ℓ. On each of the $q+1-t$ points of $\ell \setminus \mathcal{P}_0$ we see exactly t distinct $\mathcal{T}$-lines and at least $q+1-t$ more through P (since the bad lines are in $\mathcal{L}_0$). Thus $|\mathcal{L}_0| \geq (q+1-t)t+q+1-t$. Compared with the upper bound $|\mathcal{L}_0| \leq t(q+\sqrt{q}+1)$ (Theorem 3.3.5), $q \leq t(\sqrt{q}+1)+(t+1)(t-1)$ follows. By $t \leq \sqrt{q}/2$ we get $q/4 \leq \sqrt{q}/2-1$, a contradiction. $\square$

PROPOSITION 3.3.18 ([E]). *Suppose $3 \leq t \leq \sqrt{q}/2$. Then the number of $\mathcal{T}$-complete points is at most t, and the number of $\mathcal{T}$-complete lines is at most t.*

Proof. By duality it is enough to prove the proposition for points. Suppose to the contrary that there exist $t+1$ distinct $\mathcal{T}$-complete points. Then the number of $\mathcal{T}$-lines through these is at least $(t+1)(q+1)-\binom{t+1}{2}$, thus by Theorem 3.3.5 $(t+1)(q+1)-\binom{t+1}{2} \leq t(q+\sqrt{q}+1)$. This gives $2(q+1) \leq t(t+2\sqrt{q}+1)$, which contradicts $t \leq \sqrt{q}/2$. $\square$

COROLLARY 3.3.19 ([E]). *The number of points with large index is at most t. Dually, the number of lines with large index is at most t.*

Proof. Follows immediately from Propositions 3.3.17 and 3.3.18. $\square$

The following proposition shows a crucial property of points and lines with large index, which is a typical corollary of the Szőnyi–Weiner Lemma.

PROPOSITION 3.3.20 ([E]). *Suppose $t \leq \sqrt{q}/2$. Then the points with large index block the bad lines (that is, every bad line is incident with at least one point with large index). Dually, lines with large index cover the bad points.*

Proof. Again, by duality it is enough to prove the proposition for points. Suppose to the contrary that there exists a bad line ℓ on which every point has index at most c, where $c \leq t$, and suppose that there exists a point P on ℓ with $\mathrm{ind}(P) = c$. Then the total number δ of bad lines counted through the points of ℓ is at most $(c-1)(q+1)+1$. Then using inequality (3.1) from the proof of Proposition 3.3.15 we get

$$0 \leq c^2 - c(q+1) + (c-1)(q+1) + 1 = c^2 - q,$$

a contradiction since $c \leq t < \sqrt{q}$. $\square$

Note that if $t \not\equiv 1 \pmod p$, then the existence of a point with large index is equivalent to the existence of a line with large index (if t is small enough to use the propositions). For instance a point P with large index is $\mathcal{T}$-complete (Proposition 3.3.17), that is, all lines through it are in $\mathcal{T}$, hence the number of $\mathcal{T}$-lines through it is $1 \pmod p$, thus P is bad. On this bad point there should exist a line with large index (Proposition 3.3.20).

PROPOSITION 3.3.21 ([E]). *Suppose that $3 \leq t \leq \sqrt{q}/2$ and also $t \leq p$. Then the line joining two $\mathcal{T}$-complete points has large index. Dually, the intersection point of two $\mathcal{T}$-complete lines has large index.*

Proof. Once more, by duality it is enough to prove the proposition for points. Let P_1 and P_2 be two $\mathcal{T}$-complete points and denote by ℓ the line joining them. Then $\ell \in \mathcal{L}_0$. As $3 \leq t \leq p$, $q+1 \not\equiv t \pmod p$, hence P_1 and P_2 are bad. Suppose to the contrary that the index of ℓ is at most t. Then there are at least $q+1-t$ good points on ℓ, each having $t \mod p$, thus at least t $\mathcal{T}$-lines through them (here we use $t \leq p$ and ℓ being a $\mathcal{T}$-line). Counting the $\mathcal{T}$-lines through the good points of ℓ, P_1, and P_2, we can deduce that $|\mathcal{L}_0| \geq (q+1-t)(t-1) + 2q + 1$. Compared with the upper bound $|\mathcal{L}_0| \leq t(q + \sqrt{q} + 1)$ (Theorem 3.3.5), we get $q \leq t(\sqrt{q}+1) + t^2$. This contradicts $t \leq \sqrt{q}/2$ whenever $q > 4$, which follows from the assumption $3 \leq t \leq \sqrt{q}/2$. $\square$

COROLLARY 3.3.22 ([E]). *Suppose that $3 \leq t \leq \sqrt{q}/2$ and also $t \leq p$. Let $\mathcal{P}'$ be either the set of $\mathcal{T}$-complete points or the set of points with large index. Let $\mathcal{L}'$ be either the set of $\mathcal{T}$-complete lines or the set of lines with large index. Then $(\mathcal{P}', \mathcal{L}')$ is a degenerate subplane.*

Proof. We only need to check whether the intersection of two lines of $\mathcal{L}'$ is in $\mathcal{P}'$, and if the line joining two points of $\mathcal{P}'$ is in $\mathcal{L}'$. As points and lines with large index are $\mathcal{T}$-complete (Proposition 3.3.17), this follows from Proposition 3.3.21 in all the four cases. As $|\mathcal{P}'| \leq t \leq p$ by Proposition 3.3.18 or Corollary 3.3.19, the subplane must be degenerate. □

In case of a complete subplane (Construction 3.3.1), the subplane formed by the $\mathcal{T}$-complete points and lines has t points and t lines, while in the union of t disjoint Baer subplanes (Construction 3.3.2) it is empty. In the proof of Theorem 3.3.11, we will verify this property with the help of weighted t-fold blocking sets.

PROPOSITION 3.3.23 ([E]). *Suppose that $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ is a t-PDS in* $\mathrm{PG}(2, q)$*, $3 \leq t \leq \sqrt{q}/2$, and $t \leq p$. Giving weight t to points with large index and weight one to the other points of $\mathcal{P}_0$, we obtain a weighted t-fold blocking set. The analogous dual statement for lines holds as well.*

Proof. By Proposition 3.3.20, there is at least one point with large index (of weight t) on each bad line. On the other hand, every good line is a $t \pmod p$ secant to $\mathcal{P}_0$, thus by $t \leq p$ and $\mathcal{P}_0$ being a blocking set (Proposition 3.3.6), a good line intersects $\mathcal{P}_0$ in a positive number of, hence in at least t points. □

REMARK 3.3.24. *If there are no points (and thus lines) with large index, then the above proposition yields that $\mathcal{P}_0$ is a t-fold blocking set (without weights).*

Now we are ready to prove the main result of this chapter.

Proof of Theorem 3.3.11 ([E]). Recall that the assumptions on t (besides $3 \leq t \in \mathbb{N}$) are the following: if $q = p^h$, then assume $t < p^{1/2}/2$ for $h = 1, 2$, and $t < \min\left\{p + 1, c_p q^{1/6} - 1, q^{1/4}/2\right\}$ for $h \geq 3$, where $c_2 = c_3 = 2^{-1/3}$ and $c_p = 1$ for $p > 3$. At this point we have to assume a somewhat stronger bound on t in case of $h = 1$, say, $t < \sqrt{q}/3$, mainly to satisfy the conditions of Result 1.5.12. Later we will refine the proof so that the original bound will be enough.

STEP 1: *$\mathcal{T}$ contains k $\mathcal{T}$-complete points and lines and $t - k$ Baer subplanes for some k ($0 \leq k \leq t$), which will be seen to be well defined in Step 2.*

By Proposition 3.3.3 we have $|\mathcal{P}_0| = |\mathcal{L}_0| \geq t(q+1-t) = tq+t-t^2$. The number of $\mathcal{T}$-complete points is at most t (Proposition 3.3.18), thus giving weight t to the points with large index (which are $\mathcal{T}$-complete by Proposition 3.3.17) we obtain a weighted t-fold blocking set $\mathcal{P}_0^w$ (Proposition 3.3.23) with $|\mathcal{P}_0^w| \leq |\mathcal{P}_0| + t(t-1) \leq tq + t + t(\sqrt{q} + t - 1)$ (Theorem 3.3.5), in which at least $|\mathcal{P}_0| - t \geq tq - t^2$ points

are simple. Dually, giving weights analogously to the lines of $\mathcal{L}_0$ we obtain a weighted t-fold covering set $\mathcal{L}_0^w$. The assumptions on t and q yield that we may use Results 1.5.12 and 1.5.13 together with their duals to see that $\mathcal{P}_0^w$ contains the sum of the point-sets of k lines $\ell_1, \ldots, \ell_k$ and $t-k$ Baer subplanes $B_1^P, \ldots, B_{t-k}^P$, while $\mathcal{L}_0^w$ contains the sum of the line-sets of k' points $P_1, \ldots, P_{k'}$ and $t-k'$ Baer subplanes $B_1^L, \ldots, B_{t-k'}^L$. (Here a subplane is considered as a pair of a point-set and a line-set.)
Note that by the definitions of $\mathcal{P}_0^w$ and $\mathcal{L}_0^w$, the only points and lines in $\mathcal{P}_0^w$ and $\mathcal{L}_0^w$ with weight more than one are those with large index, which are $\mathcal{T}$-complete as well (Proposition 3.3.17).
Let $\mathcal{P}^* = \{P_1, \ldots, P_{k'}\}$, $\mathcal{B}_L^* = \{B_1^L, \ldots, B_{t-k'}^L\}$, $\mathcal{L}^* = \{\ell_1, \ldots, \ell_k\}$, and $\mathcal{B}_P^* = \{B_1^P, \ldots, B_{t-k}^P\}$. Note that the elements of $\mathcal{P}^*$ and $\mathcal{L}^*$ are $\mathcal{T}$-complete. Moreover, as the line-set of a Baer subplane $B \in \mathcal{B}_L^*$ is in $\mathcal{L}_0$ and it covers all the points of B $\sqrt{q}+1 > t$ times, the point-set of B is contained in $\mathcal{P}_0$ (and dually as well). However, in principle it could happen that $B \notin \mathcal{B}_P^*$. Next we show that this is not the case.

STEP 2: *There are no other $\mathcal{T}$-complete points, $\mathcal{T}$-complete lines, or Baer subplanes contained in $\mathcal{T}$ than the above found ones.*

Let S be a line or a Baer subplane whose point-set is contained in $\mathcal{P}_0$. We show that $S \in \mathcal{L}^*$ or $S \in \mathcal{B}_P^*$. Suppose to the contrary. Then the union of the point-sets of the elements of $\mathcal{L}^*$ and $\mathcal{B}_P^*$ contains at least $t(q+1) - t(t-1)$ points (in $\mathcal{P}_0$, without multiplicities), as any one of them has at least $q+1$ points, and at most t points may be in more than one of them (as $\mathcal{P}_0^w$ contains their sum, and there are at most t points with weight more than one in $\mathcal{P}_0^w$). Recall that the intersection of two lines, a line and a Baer subplane, or two Baer subplanes contains at most 1, $\sqrt{q}+1$, or $\sqrt{q}+2$ points, respectively. Thus, as $|S| \geq q+1$, S adds at least $(q+1) - t(\sqrt{q}+2)$ new points to the union, whence $|\mathcal{P}_0| \geq (t+1)(q+1) - t(t-1) - t(\sqrt{q}+2)$. Compared with the upper bound $|\mathcal{P}_0| \leq t(q+\sqrt{q}+1)$ (Theorem 3.3.5) and considering the assumed upper bounds on t, we get a contradiction. Together with the dual of this argument, we obtain the stated result, which yields $\mathcal{B}_L^* = \mathcal{B}_P^*$ and $k = k'$.

STEP 3: $k = 0$ *or* $k = t$.

Suppose to the contrary that there is a $\mathcal{T}$-complete line ℓ and a Baer subplane B as well in $\mathcal{T}$. As (the point-set of) a Baer subplane is a blocking set, there exists a point P in $\ell \cap B$. As $\ell \in \mathcal{L}^*$ and $B \in \mathcal{B}_P^*$, P has weight at least two in $\mathcal{P}_0^w$.

Thus P has large index, hence it is $\mathcal{T}$-complete (Proposition 3.3.17), consequently $P \in \mathcal{P}^*$. Therefore, as $B \in \mathcal{B}_L^*$ also holds, $\mathcal{L}_0^w$ contains the sum of the line-sets of P and B, thus the $\sqrt{q}+1 > t$ lines through P belonging to B have weight at least two in $\mathcal{L}_0^w$, hence they are $\mathcal{T}$-complete. However, the number of $\mathcal{T}$-complete lines is at most t (Proposition 3.3.18), a contradiction.

STEP 4: *$\mathcal{T}$ is a complete subplane or the union of t disjoint Baer subplanes.*

Recall that $\mathcal{T}$-complete points and lines form a subplane (Corollary 3.3.22). As $k = 0$ or $k = t$, then $\mathcal{T}$ either contains the union of t disjoint Baer subplanes (as $\mathcal{P}_0^w$ contains the sum of the Baer subplanes, a point in the intersection would have weight at least two, hence it would be $\mathcal{T}$-complete) or a $\mathcal{T}$-complete subplane $(\mathcal{P}^*, \mathcal{L}^*)$ on t points and lines, which is degenerate as $t \le p$. Both of these are t-PDSs, thus $\mathcal{T}$ contains a t-PDS $\mathcal{T}'$. By Proposition 3.3.9, this may happen only if $\mathcal{T} = \mathcal{T}'$. □

Refining the proof of Theorem 3.3.11 for $q = p$ prime

If $q = p$ prime, then we can avoid referring to the cited results on weighted t-fold blocking sets. Supposing $q = p$ prime and $t \ge 2$, every good line (a $t \mod p$ secant) must intersect $\mathcal{P}_0$ in exactly t points, which is quite a strong property, yet not enough in itself: we will use Lemma 2.1.6. This subsection is also based on [E].

We assume $3 \le t < \sqrt{p}/2$. Recall that the points and lines with large index (which are $\mathcal{T}$-complete) form a subplane, which must be degenerate as we are in $\mathrm{PG}(2,p)$, and that the number of $\mathcal{T}$-complete points (and lines) is at most t; moreover, bad lines are blocked by points with large index (see Propositions 3.3.17, 3.3.18, 3.3.20, 3.3.22).

CASE 1: *there are no points or lines with large index.*

Then every line is good, hence intersects $\mathcal{P}_0$ in exactly t points. But then counting the points of $\mathcal{P}_0$ through the lines incident with a point inside or outside $\mathcal{P}_0$ we get that $|\mathcal{P}_0| = 1 + (t-1)(q+1)$ and $|\mathcal{P}_0| = (q+1)t$, a contradiction.

CASE 2: *the points and lines with large index form a subplane of type π_1.*

Then there exists an incident point-line pair (P, ℓ), both having large index, such that every line with large index goes through P and dually, every point with large index lies on ℓ. Take a line e through P with small index. Then every point Q on e except P is good (since the bad ones are blocked by the lines with large index, each of which intersects e in P), hence there are exactly t $\mathcal{T}$-lines through it. Thus there are $t-1$ $\mathcal{T}$-lines through Q different from PQ. We may choose the coordinate system in such a way that the line at infinity has large index and P is the common point of vertical lines. Then the non-vertical $\mathcal{T}$-lines cover all the points of the affine plane exactly $t-1$ times, except possibly the points of $t-1$ vertical lines with large index. Applying Lemma 2.1.6 for the above situation, we get that there is a unique line with large index that contains $t-1$ $\mathcal{T}$-complete points (besides P) and that every point out of this line is good. Thus this line is the only line that has more than one bad point on it, i.e., this line is ℓ. It follows from duality that P is the only point with large index and it has $t-1$ $\mathcal{T}$-complete lines through it (besides ℓ). It is straightforward that this construction is what we get from Construction 3.3.1 starting with a degenerate subplane of type π_1.

CASE 3: *the points and lines with large index form a subplane of type π_2.*

Denote the points with large index by $P_1, \ldots, P_k$ $(k \leq t)$ in such a way that $P_2, \ldots, P_k$ all lie on a line ℓ, but $P_1 \notin \ell$. Here $k \neq 2$ may be assumed, as otherwise the degenerate subplane in question is of type π_1 as well.

Pick a point P on ℓ with small index and denote by c the number of $\mathcal{T}$-points on the line PP_1 besides P and P_1. Counting the elements of $\mathcal{P}_0$ from P we get that $|\mathcal{P}_0| = q+1+(t-1)(q-1)+c+1$ $(*)$, as there are $q+1$ $\mathcal{T}$-points on ℓ, $t-1$ further $\mathcal{T}$-points on the $q-1$ good lines through P not incident with P_1 and $c+1$ more points on the line PP_1 (note that by Proposition 3.3.20 the only possibly bad lines through P are ℓ and PP_1). This implies that c must be independent from the choice of P. Counting the $\mathcal{T}$-points via the lines passing through P_1 we get that $|\mathcal{P}_0| = 1+(k-1)(q-1)+(q+1)+c(q+1-(k-1))$ $(**)$. Rearranging the equation obtained from $(*)$ and $(**)$ we get $c(k-2) = (c+k-t)(q-1)$.

If $k = 1$, then $-c = (c+1-t)(q-1)$, hence by $c \leq q-1$ we get either $c = 0$ and $t = 1$, or $c = q-1$ and $t = q+1$. The latter case is out of interest, the first corresponds to complete subplane of type π_2 (which is an antiflag in this case).

If $k \geq 3$, then by $c \leq q-1$, we need to have $k-2 \geq c+k-t$, hence $c \leq t-2$. Using this and $k \leq t$, we get that $(c+k-t)(q-1) = c(k-2) \leq (t-2)^2 < q-1$ by the assumptions. Hence the only possibility is that $c+k-t = 0$, whence $c = 0$ and $k = t$ follows. It is easy to see that this implies that the pair $(\mathcal{P}_0, \mathcal{L}_0)$ is exactly the complete degenerate subplane of type π_2 spanned by the t points with large index. $\square$

3.4 Perfect dominating sets in generalized quadrangles

In contrast with the case of projective planes, not much is known about t-fold perfect dominating sets in generalized quadrangles. From now on we consider a GQ $(\mathcal{P}, \mathcal{L})$ of order q. The constructions we are to present here are based on the ideas of [D], though we have rephrased them using the (already presented) more general concepts of [C].

DEFINITION 3.4.1. *For a point-set* $\mathcal{U} \subset \mathcal{P}$, $\mathcal{U}^{\perp}$ *denotes the set of points collinear with all points of* U *(every point is considered to be collinear with itself). One can analogously define* $\mathcal{W}^{\perp}$ *for a set* $\mathcal{W}$ *of lines.*

It is easy to see that for any pair of points $\{U, V\}$, $\left|\{U, V\}^{\perp}\right| = q + 1$. Note that if U and V are collinear, then $\{U, V\}^{\perp}$ is the point-set of the line connecting U and V, while if U and V are not collinear, then $\{U, V\}^{\perp}$ consists of pairwise non-collinear points.

DEFINITION 3.4.2. *A non-collinear point-pair* U, V *is called* regular *if it satisfies* $\left|\{U, V\}^{\perp\perp}\right| = q + 1$. *The definition of a regular line-pair is analogous.*

DEFINITION 3.4.3. *An* ovoid *in a GQ of order* q *is a set of* $q^2 + 1$ *points that intersects every line in exactly one point. A* spread *is the dual of an ovoid; that is, a set of* $q^2 + 1$ *lines that cover all points exactly once.*

Next we construct some $(1, 0)$ and $(0, 1)$-PDSs (see Definition 3.2.5). Recall that Corollary 3.2.8 claims that the union of a $(0, 1)$-PDS and a $(1, 0)$-PDS is a 1-PDS.

PROPOSITION 3.4.4.

1. *Let* $\mathcal{S}$ *be a spread. Then* $(\emptyset, \mathcal{S})$ *is a* $(1, 0)$*-PDS of size* $(0, q^2 + 1)$.
2. *Let* ℓ *be any line. Then the ball* $B(\ell, 2)$ *is a* $(1, 0)$*-PDS of size* $(q + 1, q^2 + q + 1)$.
3. *Let* $\{U, V\}$ *be a regular point-pair,* $\mathcal{P}_0 = \{U, V\}^{\perp} \cup \{U, V\}^{\perp\perp}$, *and let* $\mathcal{L}_0$ *consist of the lines that intersect* $\mathcal{P}_0$. *Then* $\mathcal{T} = (\mathcal{P}_0, \mathcal{L}_0)$ *is a* $(1, 0)$*-PDS of size* $(2q + 2, q^2 + 2q + 1)$.

The duals of the above $(1, 0)$*-PDSs are* $(0, 1)$*-PDSs.*

Proof. Parts 1. and 2. are straightforward, so we only verify part 3. By its definition, a line $\ell \notin \mathcal{L}_0$ does not intersect $\mathcal{P}_0$, so we only have to check whether every point $P \notin \mathcal{P}_0$ is covered by exactly one line of $\mathcal{L}_0$. As U and V are not collinear, $\{U,V\}^\perp$ and $\{U,V\}^{\perp\perp}$ both consist of $q+1$ pairwise non-collinear points. As any point of $\{U,V\}^\perp$ is collinear with any point of $\{U,V\}^{\perp\perp}$, it is easy to see that $\mathcal{L}_0 = \cup_{Q\in\{U,V\}^\perp}[Q] = \cup_{Q\in\{U,V\}^{\perp\perp}}[Q]$, and that the intersection of two lines of $\mathcal{L}_0$ is in $\{U,V\}^\perp$ or $\{U,V\}^{\perp\perp}$. Hence $\mathcal{L}_0$ covers all the $(q+1)^2(q-1) = q^3+q^2+q+1-|\mathcal{P}_0|$ points not in $\mathcal{P}_0$ exactly once. □

For more information and details about GQs we refer to the book [60]. There one can find that in the classical generalized quadrangle $Q(4,q)$, there exists a regular line-pair and an ovoid for all prime power q, and there exists a regular point-pair and a spread if and only if q is even.

PROPOSITION 3.4.5 ([D]). *If q is odd, then there is a 1-PDS of size q^2+3q+1 in $Q(4,q)$. If $q>2$ is even, then there is a 1-PDS of size q^2+4q+3 in $Q(4,q)$.*

Proof. If q is an odd prime power, we may unite a $(0,1)$-PDS obtained from a regular line-pair $\{e,f\}$ of $Q(4,q)$ and a ball $B(\ell,2)$ with $\ell \notin \{e,f\}^\perp \cup \{e,d\}^{\perp\perp}$ to obtain a 1-PDS of size q^2+3q+1. If q is an even prime power, then one can find a regular point-pair and a regular line-pair in $Q(4,q)$ such that the $(0,1)$ and the $(1,0)$-PDSs derived from them as in Proposition 3.4.4 are disjoint, hence the constructed 1-PDS is of size q^2+4q+3. In case of $q=2$, this would be the whole GQ, so we need $q>2$. □

No characterization results are known for t-PDSs in GQs, not even for $t=1$. Beukemann and Metsch [20] studied 1-PDSs in arbitrary generalized quadrangles of order q, and in particular, in $Q(4,q)$. They give several examples, some of which can be obtained as the union of some $(0,1)$ and $(1,0)$-PDSs above as well, and they find a sporadic example of size $22 > q^2+3q+1$ in $Q(4,3)$. They prove the following upper bound on the size of a 1-PDS in a GQ, which is almost the double of the size of the largest construction known.

RESULT 3.4.6 (Beukemann–Metsch [20]). *Let Q be a generalized quadrangle of order q, $q>1$, and let $\mathcal{T}$ be a 1-PDS in Q. Then*

1. $|\mathcal{T}| \le 2q^2+2q-1$;

2. *If Q is $Q(4,q)$ and q is even, then* $|\mathcal{T}| \le 2q^2+q+1$.

Beukemann and Metsch also have results on the size of a smallest 1-PDSs. However, it seems that understanding t-PDSs in GQs is much more difficult than in projective planes. In the latter case the characterization of 1-PDSs is almost immediate, as seen in Theorem 3.3.7.

3.5 Various methods, same results

In this section, based on [C], we examine some constructions in various articles and show their relations.

Brown [25] (1967) obtained $(k,6)$-graphs on $2kq$ vertices by deleting a $(q+1-k)$-PDS from an arbitrary projective plane of order q, $q \geq k$. In fact, he deleted a complete degenerate subplane of type π_1 (cf. Construction 3.3.1). From the Moore bound and the distribution of primes it follows that $c(k,6) \sim 2k^2$. Brown's method can be regarded as a combinatorial, geometric approach.

In 1997, Lazebnik, Ustimenko, and Woldar [56] proved the following.

RESULT 3.5.1. *Let $k \geq 2$ and $g \geq 5$ be integers, and let q denote the smallest odd prime power for which $k \leq q$. Then*

$$c(k,g) \leq 2kq^{\frac{3}{4}g-a},$$

where $a = 4,\ 11/4,\ 7/2,\ 13/4$ for $g \equiv 0,\ 1,\ 2,\ 3 \pmod 4$, respectively.

In particular, for $g = 6, 8, 12$ this gives $c(k,6) \leq 2kq$, $c(k,8) \leq 2kq^2$, $c(k,12) \leq 2kq^5$, where q is the smallest odd prime power not smaller than k. Combined with the Moore bound, this yields $c(k,8) \sim 2k^3$.

The construction in the background is the following. First they construct an incidence structure $D(q)$ as follows. Points and lines of $D(q)$ are written inside a parenthesis () and angle brackets $\langle\rangle$, respectively. Consider the vectors (P) and $\langle \ell \rangle$ of infinite length over GF(q):

$$\begin{aligned} (P) &= (p_1, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, p_{23}, \ldots, p_{ii}, p'_{ii}, p_{i,i+1}, p_{i+1,i}, \ldots), \\ \langle \ell \rangle &= \langle \ell_1, \ell_{11}, \ell_{12}, \ell_{21}, \ell_{22}, \ell'_{22}, \ell_{23}, \ldots, \ell_{ii}, \ell'_{ii}, \ell_{i,i+1}, \ell_{i+1,i}, \ldots \rangle . \end{aligned}$$

A point (P) and a line $\langle \ell \rangle$ are incident if and only if the following infinite list of equations hold simultaneously:

$$\begin{aligned}
\ell_{11} - p_{11} &= \ell_1 p_1 \\
\ell_{12} - p_{12} &= \ell_{11} p_1 \\
\ell_{21} - p_{21} &= \ell_1 p_{11} \\
\ell_{ii} - p_{ii} &= \ell_1 p_{i-1,i} \\
\ell'_{ii} - p'_{ii} &= \ell_{i-1,i} p_1 \\
\ell_{i,i+1} - p_{i,i+1} &= \ell_{i,i} p_1 \\
\ell_{i+1,i} - p_{i+1,i} &= \ell_1 p'_{ii},
\end{aligned}$$

where the last four equations are defined for all $i \geq 2$. For an integer $n \geq 2$, let $D(n,q)$ be derived from $D(q)$ by projecting every vector onto its initial n coordinates. Then the point-set $\mathcal{P}_n$ and the line-set $\mathcal{L}_n$ of $D(n,q)$ both have q^n elements, and incidence is defined by the first $n-1$ equations above. Note that those involve only the first n coordinates of (P) and $\langle \ell \rangle$, hence apply to the points and lines of $D(n,q)$ unambiguously. $D(n,q)$ as a bipartite graph can be proved to be q-regular and have girth at least $n+4$ (thus at least $n+5$ if n is odd).

Let $R, S \subset \mathrm{GF}(q)$, where $|R| = r \geq 1$ and $|S| = s \geq 1$, and let

$$\mathcal{P}_R = \{(P) \in \mathcal{P}_n \colon p_1 \in R\}, \mathcal{L}_S = \{\langle \ell \rangle \in \mathcal{L}_n \colon \ell_1 \in S\}.$$

The graph $D(n,q,R,S)$ is defined as the subgraph of $D(n,q)$ induced by $\mathcal{P}_R \cup \mathcal{L}_S$. It can be shown that every vertex in $\mathcal{P}_R$ or $\mathcal{L}_S$ in $D(n,q,R,S)$ has degree s or r, respectively.

In the case $n = 2$, $\mathcal{P}_2 = \{(p_1, p_{11}) \in \mathrm{GF}(q)^2\}$ and $\mathcal{L}_2 = \{\langle \ell_1, \ell_{11} \rangle \in \mathrm{GF}(q)^2\}$, and a point $(x,y) \in \mathcal{P}_2$ is incident with the line $\langle m, b \rangle \in \mathcal{L}_2$ if and only if $b - y = mx$. Let

$$\begin{aligned}
\varphi \colon D(2,q) &\to \mathrm{AG}(2,q) \\
(x,y) &\mapsto (x,y) \\
\langle m, b \rangle &\mapsto \{(x,y) \colon y = -mx + b\}.
\end{aligned}$$

The mapping φ is clearly injective and preserves incidence, hence it is an embedding of $D(2,q)$ into $\mathrm{AG}(2,q) \subset \mathrm{PG}(2,q)$. Note that vertical lines are not in the image, hence $\varphi(D(2,q))$ can be obtained by deleting the ideal line together with its points and the vertical lines from $\mathrm{PG}(2,q)$. If we consider the induced subgraph $D(2,q,R,S)$, geometrically it means that we take points only on the vertical lines $X = x$ with $x \in R$ and lines with slopes $-m \in S$. In other words, we delete (besides the formerly deleted points and lines) all the points of the vertical lines $X = x$ with $x \notin R$, and we delete all lines having slopes $-m \notin S$; that is, we delete the lines that intersect the ideal line in a direction (or point) (m) with $-m \notin S$. Hence the deleted objects form an (r, s)-PDS obtained from a degenerate subplane of type π_1 on s points and r lines.

To see why the construction for $n = 3$ (that is, $g = 8$) is isomorphic to an (s, t)-good structure in a GQ, we give an explicit description of $\mathrm{PG}(3, q)$ and the classical generalized quadrangle $W(q)$ first. We use homogeneous coordinates as introduced in Chapter 1. A line ℓ of $\mathrm{PG}(3, q)$ corresponds to a plane of $\mathrm{GF}(q)^4$, and hence can be defined as the span of two vectors; that is, $\ell = \{\alpha(x : y : z : w) + \beta(x' : y' : z' : w') \mid (\alpha, \beta) \in \mathrm{GF}(q)^2 \setminus \{(0, 0)\}\}$ for some distinct points $(x : y : z : w)$ and $(x' : y' : z' : w')$ of $\mathrm{PG}(3, q)$. The generalized quadrangle $W(q)$ is defined by a non-degenerate symplectic form over $\mathrm{PG}(3, q)$. Let q be an odd prime power. Take a matrix $A \in \mathrm{GF}(q)^{4\times4}$ such that $A^T = -A$, and for $x, y \in \mathrm{GF}(q)^4$, let $x \sim y$ (in words, x is perpendicular to y) if and only if $xAy^T = 0$. Note that the relation $\sim$ is well defined over $\mathrm{PG}(3, q)$, and for all $x \in \mathrm{GF}(q)^4$ we have $x \sim x$. The points of $W(q)$ are those of $\mathrm{PG}(3, q)$, and the lines of $W(q)$ are those of $\mathrm{PG}(3, q)$ that are totally isotropic; that is, any two points of which are perpendicular. Note that if $x \sim y$, then $(\alpha x+\beta y) \sim (\gamma x+\delta y)$ for all $\alpha, \beta, \gamma, \delta \in \mathrm{GF}(q)$, hence two points x and y are collinear in $W(q)$ if and only if $x \sim y$. Thus a point is incident with a line in $W(q)$ if and only if it is perpendicular to at least two of its points (and hence to all of them). It can be proved that $W(q)$ is a generalized quadrangle of order (q, q).

Now the graph $D(3, q)$ has point-set $\mathcal{P}_3 = \{(x, y, z) \in \mathrm{GF}(q)^3\}$ and line-set $\mathcal{L}_3 = \{\langle a, b, c\rangle \in \mathrm{GF}(q)^3\}$, where $(x, y, z) \in \langle a, b, c\rangle$ if and only if $b - y = ax$ and $c - z = bx$. Let

$$\begin{aligned}
\varphi\colon D(3, q) &\to \mathrm{PG}(3, q)\\
(x, y, z) &\mapsto (x : y : z : 1)\\
\langle a, b, c\rangle &\mapsto \{\alpha(1 : -a : -b : 0) + \beta(0 : b : c : 1) \mid (\alpha, \beta) \in \mathrm{GF}(q)^2 \setminus \{(0, 0)\}\},
\end{aligned}$$

furthermore, let

$$A = \begin{pmatrix} 0 & 1 & 0 & 0\\ -1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 1 & -1 & 0 \end{pmatrix}.$$

We claim that φ is an embedding of $D(3,q)$ into $W(q)$ defined by the symplectic form coming from A. It is clear that φ is injective. Moreover, $(x,y,z) \in \langle a,b,c\rangle \iff b-y=ax$ and $c-z=bx \iff (x:y:z:1)A(1:-a:-b:0)=0$ and $(x:y:z:1)A(0:b:c:1)=0 \iff (x:y:z:1)$ is on the line spanned by $(1:-a:-b:0)$ and $(0:b:c:1)$, hence φ preserves incidence.

Note that the q^2+q+1 points collinear with $P_1=(0:0:1:0)$ in $W(q)$ (that is, points of form $(x:y:z:0)$, or in other words, the points of the plane at infinity) are not in the image of φ; moreover, lines intersecting the line $\ell_1=\{(0:\alpha:\beta:0)\}$ are also excluded (no lines in the image contain a point with first and fourth coordinates both zero). This means that $\varphi(D(3,q)) \subset W(q)$ is obtained from $W(q)$ by deleting every point collinear with P_1 and every line intersecting ℓ_1. As $P_1 \in \ell_1$, this corresponds to a neighboring balls construction with center-set $(\{P_1\},\{\ell_1\})$. The points $(x:y:z:1)$ with $x \notin R$ fixed are precisely the q^2 points collinear to $P_x=(0:1:x:0) \in \ell_1$ not on ℓ_1. The lines $\{\alpha(1:-a:-b:0)+\beta(0:b:c:1)\}$ with $a \notin S$ fixed are precisely the q^2 lines intersecting the line $\ell_a=\{\gamma(1:-a:0:0)+\delta(0:0:1:0)\}$ not in P_1. Hence $\varphi(D(3,q,R,S))$ can be obtained by deleting the balls around $\mathcal{P}^*=\{P_x\colon x \notin R\}\cup\{P_1\}$ and $\mathcal{L}^*=\{\ell_a\colon a\notin S\}\cup\{\ell_1\}$. Hence these constructions, coming from a more algebraic approach, are indeed special cases of Brown's method.

Using the addition and multiplication tables of $\mathrm{GF}(q)$, Abreu, Funk, Labbate and Napolitano ([2], 2006) constructed two infinite families of $(k,6)$ graphs, $k \le q$, via their adjacency matrices. The number of vertices of the graphs in the first and the second family are $2kq$ and $2(kq+(q-1-k))$, respectively. The second construction yields a graph smaller than the previously known ones for $k=q$, resulting $c(q,6) \le 2(q^2-1)$ for any prime power q. In the sequel we show that these families of Abreu et al. [2] are equivalent to deleting a $(q+1-k)$-PDS from $\mathrm{PG}(2,q)$ with an underlying degenerate subplane of type π_1 or π_2, respectively. Thus the first family was a reinvention of Brown's construction [25], though the two approaches are different. Note that, however, Abreu et. al. start from $\mathrm{PG}(2,q)$, while Brown's construction works in arbitrary projective planes.

Let us consider and rephrase the constructions of [2]. Let $A=A(q)$ be the addition table of the finite field $\mathrm{GF}(q)$, i.e., the rows and columns are indexed by the elements of the field, and $A_{i,j}=i+j$. Similarly, let $M=M(q)$ be the multiplication table of the multiplicative group $\mathrm{GF}(q)^*$ of $\mathrm{GF}(q)$, i.e., $M_{i,j}=ij$. Let H be an arbitrary matrix over $\mathrm{GF}(q)$ and let $z \in \mathrm{GF}(q)$. Define the $0-1$ position matrix $P_z(H)$ of z in H by $P_z(H)_{i,j}=1$ if and only if $H_{i,j}=z$. Now the matrices corresponding to the two constructions $G_*(q,1)$ and $G_+(q,1)$ of [2, page 126] are the following: substitute every element $M_{i,j}$ by $P_{M_{i,j}}(A)$ in M, and respectively, substitute every element $A_{i,j}$ by $P_{A_{i,j}}(M)$ in A. Let these "blow ups" be denoted by $\overline{M}$ and $\overline{A}$, respectively. Let us consider $\overline{M}$. It is natural to index its rows and columns by pairs (a,b), $a \in \mathrm{GF}(q)^*$, $b \in \mathrm{GF}(q)$. By its definition, $\overline{M}_{(x,y),(m,b)} = 1$ exactly when $xm = y + b$. Now we can see that the rows and columns of $\overline{M}$ naturally correspond to the points and lines of the affine plane $\mathrm{AG}(2,q)$: the row (x,y) corresponds to the point (x,y) in $\mathrm{AG}(2,q)$, while the column (m,b) corresponds to the line defined by the equation $Y = mX - b$, and a 1 entry in $\overline{M}$ corresponds to a flag. Since the first coordinates are from $\mathrm{GF}(q)^*$, we do not have lines having slope 0 or ∞ (i.e., horizontal and vertical lines), furthermore we do not have points on the y axis (the line with equation $X = 0$). Since $\mathrm{PG}(2,q)$ can be viewed as $\mathrm{AG}(2,q)$ and a line at infinity, one can see that the structure related to $\overline{M}$ comes from $\mathrm{PG}(2,q)$ by removing all the points of the line at infinity and the y axis, and all the lines through the common points of vertical and horizontal lines. The authors of [2] then complete the matrix $\overline{M}$ in a way that corresponds to adding the horizontal lines and the points on the y-axis. Also, they delete rows (x,y) and columns (m,b) of $\overline{M}$ with x and m in a fixed set $R \subset \mathrm{GF}(q)^*$. This means that they remove the lines with slope $m \in R$ (that is, lines through the points $(m) \in \ell_\infty$, $m \in R$) and points on the horizontal lines with equation $X = x$, $x \in R$. So we can see that this family can be obtained according to Construction 3.3.1 with an underlying subplane of type π_1. Similarly, it is easy to verify that $\overline{A}$ is the incidence matrix of a graph coming from Construction 3.3.1 with an underlying subplane of type π_2.

This example shows how such matrix techniques can be translated into a geometrical point of view. A construction based on Baer subplanes, similar to Construction 3.3.2, was also given in [2] using matrices, but only for $q = 4, 9, 16$. Note that there are also constructions of this kind that produce non-induced subgraphs (e.g., [10]), which topic we are to touch in Section 3.6.

Investigating a proper induced subgraph of the incidence graph of a generalized polygon, Araujo, González, Montellano-Ballesteros and Serra ([4], 2007) showed $c(k,2n) \le 2kq^{n-2}$, where $n \in \{3,4,6\}$, $k \le q$, and q is the order of a generalized n-gon. Their construction uses only elementary combinatorial properties of generalized polygons, and it can be easily seen that these constructions are directly equivalent to Construction 3.2.1; thus it may be regarded as the generalization Brown's one. The upper bound of [4] on $c(k,8)$ is the same as of Lazebnik et al.'s [56] (though the latter works only if q is an odd prime power), but the bound on $c(k, 12)$ is better, and leads to $c(k, 12) \sim 2k^5$. Note that the above results yield $c(k, 2n) \sim 2k^{n-1}$ for $n = 2, 3, 4, 6$.

3.6 Non-induced subgraphs of generalized polygons

So far we investigated induced regular subgraphs of generalized polygons in order to find small (k, g)-graphs, $g \in \{6, 8, 12\}$. Recall that for $n = 3, 4, 6$, Brown's frequently reinvented construction and its generalization (Construction 3.2.1) yields $c(k, 2n) \leq 2kq^{n-2}$, where q is the smallest integer not smaller than k for which a generalized n-gon $\mathrm{GP}_n(q)$ of order q exists. In other words, we could delete $tq^{n-2} + 1$ points and lines to obtain a $q + 1 - t$-regular induced subgraph of $\mathrm{GP}_n(q)$ $(t \geq 1)$. No better constructions are known unless $t = 1$, or $n = 3$ and q is a square prime power. However, by considering non-induced subgraphs of generalized polygons, one may obtain better results. The first such construction we know about, formulated via matrices, is due to Balbuena [10]. By deleting $tq + 2$ points, the same number of lines, and some edges, she found a $(q + 1 - t)$-regular subgraph of $\mathrm{PG}(2, q)$, though without pointing out the exact connection with $\mathrm{PG}(2, q)$. In this section we generalize this result to GQs and GHs. The construction is based on [A], though the version presented here is more compact. We are about to prove the following.

THEOREM 3.6.1 ([A]). *Suppose that a generalized n-gon of order q exists, and let $2 \leq k \leq q$. If $n \geq 4$, then $c(k, 2n) \leq 2k(q^{n-2} - q^{n-4})$; if $n = 3$, then $c(k, 2n) \leq 2kq - 2$.*

Before giving the proof, let us mention that for $k = q$, the above theorem and Construction 3.2.2 give the same result. Furthermore, in case of $n = 3$, a better result is due to Araujo-Pardo and Balbuena [5], who found a $(k, 6)$-graph on $2kq - 4$ vertices, also as a non-induced subgraph of a projective plane of order q, $3 \leq k \leq q - 1$ (so the number of deleted points is $tq + 3$, where $t = q + 1 - k$). As the following remark shows, the condition $k \leq q - 1$ is essential here.

THEOREM 3.6.2. *Let $G = (V; E)$ be a q-regular subgraph of a projective plane $\Pi_q = (\mathcal{P}, \mathcal{L})$ of order q. Then either $|\mathcal{P} \setminus V| = q + \sqrt{q} + 1$ or $|\mathcal{P} \setminus V| \leq q + 2$.*

Proof. Suppose that $V = (\mathcal{P} \setminus \mathcal{P}_0) \cup (\mathcal{L} \setminus \mathcal{L}_0)$. Then for any line ℓ not in $\mathcal{L}_0$, $|\ell \cap \mathcal{P}_0| \leq 1$; in other words, any line connecting two points of $\mathcal{P}_0$ is in $\mathcal{L}_0$. By duality, we obtain that $\Pi_0 = (\mathcal{P}_0, \mathcal{L}_0)$ is a closed system. If Π_0 is a degenerate subplane, then it has at most $q+2$ points and lines. If Π_0 is non-degenerate, then by Bruck's result (Result 1.5.2) we have $s = \sqrt{q}$ or $|\mathcal{P}_0| = s^2 + s + 1 \leq q + 1$. $\square$

In the rest of the section, we prove Theorem 3.6.1. Let $G = (V; E)$ be the incidence graph of a generalized n-gon of order q. Let xy be an edge of G, and consider the following standard partition (cf. the Moore bound):

$$\begin{aligned} X_i : &= \{v \in V : d(v,x) = i, d(v,y) = i+1\}, \\ Y_i : &= \{v \in V : d(v,y) = i, d(v,x) = i+1\}, \end{aligned}$$

where $0 \leq i \leq n-1$. As G has diameter n and girth $2n$, it is clear that these sets partition V. It is quite common to use this, so to speak, bi-rooted spanning tree of a generalized polygon. For any vertex $u \in X_i$ and $0 \leq j \leq n-1-i$, let

$$D_j(u) = \{v \in X_{i+j} : d(u,v) = j\}.$$

For a vertex $u \in Y_i$, define $D_j(u) \subset Y_{i+j}$ analogously. These sets contain the vertices that are j steps further from u with respect to the respective root. Note that $|D_j(u)| = q^j$, and the sets $\{D_j(z) : z \in X_i\}$ partition X_{i+j}. For convenience, if $j < 0$, then let $D_j(u)$ be empty, and accordingly, let $q^j = 0$. We will use the following property of generalized n-gons.

PROPOSITION 3.6.3 ([A]). *Let $1 \leq i, j \leq n-1$, $i + j \geq n$. Then for any pair of vertices $u \in X_i$ and $v \in Y_j$ there is at most one edge between the sets $D_{n-1-i}(u) \subset X_{n-1}$ and $D_{n-1-j}(v) \subset Y_{n-1}$. Moreover, if $i + j = n$, then there is exactly one edge between these sets.*

Proof. Suppose to the contrary that there are two edges between $D_{n-1-i}(u)$ and $D_{n-i-j}(v)$, say, u_1v_1 and u_2v_2. Then the walk obtained by concatenating the natural paths $u \to u_1$, u_1v_1, $v_1 \to v$, $v \to v_2$, v_2u_2, $u_2 \to u$ contains a cycle of length at most $2(n-1-i) + 2(n-1-j) + 2 = 4n - 2(i+j) - 2 \leq 2n - 2$, a contradiction.

Now suppose $i+j = n$. There are exactly $q^{n-1-i} \cdot q = q^{n-i} = q^j$ edges between $D_{n-1-i}(u)$ and Y_{n-1}. As the q^j sets $\{D_{n-1-j}(z) : z \in Y_j\}$ partition Y_{n-1} and, as seen above, there can be at most one edge between $D_{n-1-i}(u)$ and any of the sets $D_{n-1-j}(z)$, $z \in Y_j$, the equal number of sets and edges finishes the proof. $\square$

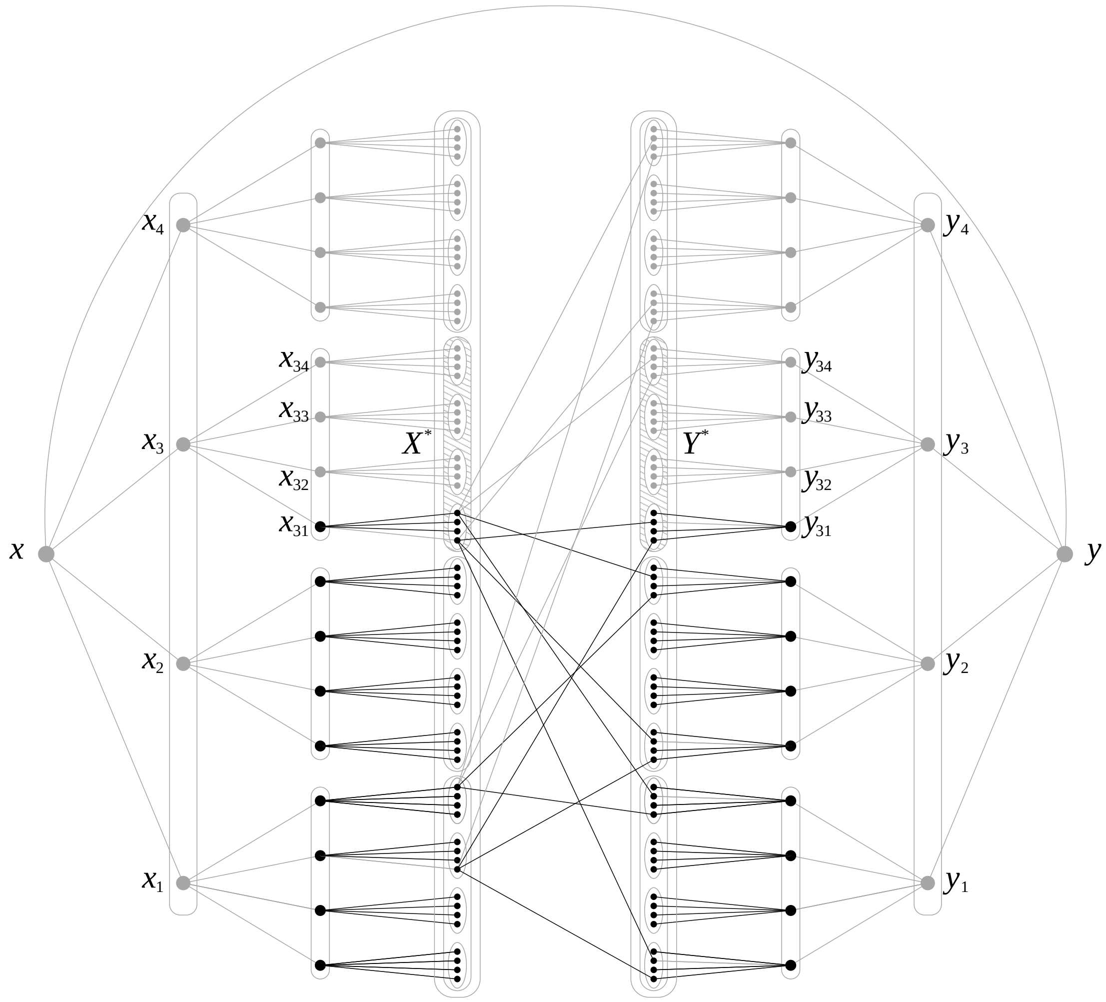

Figure 3.2: *This is a fragment of the $k = 3$-regular graph obtained from a GQ of order four. Gray objects are removed from the GQ. Only a few edges between the sets X_3 and Y_3 are depicted as an illustration.*

Please observe Figure 3.2, where the below defined sets are illustrated. Let $2 \le k \le q$, and let $X_1 = \{x_1, \ldots, x_q\}$, $Y_1 = \{y_1, \ldots, y_q\}$, $D_1(x_k) = \{x_{k1}, \ldots, x_{kq}\}$, $D_1(y_k) = \{y_{k1}, \ldots, y_{kq}\}$. Let

$$\begin{aligned}
S &:= \bigcup_{i=1}^{k-1} \bigcup_{j=n-3}^{n-2} (D_j(x_i) \cup D_j(y_i)) \cup \bigcup_{i=1}^{q-k} \bigcup_{j=n-4}^{n-3} (D_j(x_{ki}) \cup D_j(y_{ki})), \\
X^* &:= \bigcup_{i=1}^{q-k} D_{n-3}(x_{ki}) = D_{n-2}(x_k) \cap X_{n-1}, \\
Y^* &:= \bigcup_{i=1}^{q-k} D_{n-3}(y_{ki}) = D_{n-2}(y_k) \cap Y_{n-1},
\end{aligned}$$

furthermore, let

$$\begin{aligned} M: \;=\; & \{uv \in E\colon u \in X_{n-2}, v \in X_{n-1}, N(v) \cap Y^* \cap S \neq \emptyset\} \cup \\ & \{uv \in E\colon u \in Y_{n-2}, v \in Y_{n-1}, N(v) \cap X^* \cap S \neq \emptyset\}. \end{aligned}$$

Consider the subgraph H of G obtained by removing the edge-set M from the subgraph spanned by the vertices of S. We claim that H is k-regular. Let $v \in S \cap X_{n-1}$. In G, v has a unique neighbor r in X_{n-2}, and the other q neighbors are in Y_{n-1}, one in each of the sets $D_{n-2}(y_i)$ (Proposition 3.6.3). Thus v has altogether k neighbors in $S \setminus Y^*$ in G. If $N(v) \cap Y^* \neq \emptyset$, then the edge rv is in M, so v has exactly k neighbors in H. Now let $v \in S \cap X_{n-2}$. Then v has q neighbors in $S \cap X_{n-1}$. However, in G there is one edge between $D_1(v)$ and each of the sets $D_{n-3}(y_{ki})$, $1 \leq i \leq q-k$ (again by Proposition 3.6.3), thus precisely $q-k$ of these edges are missing in H, so the degree of v is again k. The analogous arguments hold for vertices in $S \cap Y_{n-1}$ and $S \cap Y_{n-2}$, so H is indeed k-regular. The number of vertices in H is $2(k-1)(q^{n-2}+q^{n-3})+2(q-k)(q^{n-3}+q^{n-4}) = 2k(q^{n-2}-q^{n-4})$ if $n \geq 4$. If $n = 3$, then $|S| = 2(k-1)(q+1)+2(q-k) = 2kq-2$. Thus Theorem 3.6.1 is proved.

3.7 Remarks

One may wonder if the upper bounds on t in Theorem 3.3.11 are necessary or sharp. The condition $t \leq p$ is mostly needed to conclude that a $t \pmod p$ secant line is a $(\geq t)$-secant. Suppose that $t = p+1$. If $|\mathcal{T}| \geq tq+2$, then $\mathcal{P}_0$ is a double blocking set by Proposition 3.3.8, so the arguments of the proof work with slight modifications, so only the case $|\mathcal{T}| \leq tq+1$ remains open. If we set $q = p^2$, Construction 3.3.3 (the points and the tangents of a unital) shows a t-PDS of size $(t-1)q+1$ different from Constructions 3.3.1 and 3.3.2. Here every line is good, but the point-set of the t-PDS is not a t-fold blocking set (cf. Remark 3.3.24). It is not clear whether there exists a $(p+1)$-PDS in $\mathrm{PG}(2,q)$, $q = p^h$, different from Constructions 3.3.1 and 3.3.2 if h is arbitrarily large.

This construction method (looking for a $(q+1-t)$-regular subgraph of a generalized n-gon of order q) is interesting mostly for $t \leq \sqrt{q}$ as usually one can find a prime k between $q-\sqrt{q}$ and $q-1$, hence a $(k+1, 2n)$ Moore cage could be chosen as the starting point as well (and it would be worth doing so).

Chapter 4

Semi-resolving sets for $\mathrm{PG}(2, q)$

In this chapter, based on [F], we discuss semi-resolving sets for projective planes. The study of this topic was motivated by a talk of Robert Bailey [7]. For further information about resolving sets and related topics, we refer to the survey of Bailey and Cameron [8].

4.1 Semi-resolving sets for $\mathrm{PG}(2, q)$

Definition 4.1.1. *Let $G = (V; E)$ be a graph, and let $H \subset V$. A vertex-set $S = \{s_1, \ldots, s_k\}$* resolves *H if for all $v \in H$ the distance list of v with respect to S, $d_S(v) = (d(v, s_1), \ldots, d(v, s_k))$, is unique.*

In other words, if S resolves H, then we can identify the vertices of H by their distances from the vertices of S. It is clear that S resolves H if and only if for all $x, y \in H$, $x \neq y$, there exists a vertex $z \in S$ such that $d(x, z) \neq d(y, z)$.

Definition 4.1.2. *Let $G = (V; E)$ be a graph. A vertex-set S is a* resolving set *for G if S resolves V. Let $G = (A, B; E)$ be a bipartite graph. A vertex-set S is a* semi-resolving set *for G if either $S \subset A$ and S resolves B, or $S \subset B$ and S resolves A.*

A (semi-)resolving set for a projective plane is that for its incidence graph. As $\mathrm{PG}(2, q)$ is self-dual, we may always assume that a semi-resolving set is a point-set which resolves the lines. However, the first couple of definitions and results are valid for arbitrary projective planes. Note that in a projective plane the distance of a point and a line is one or three depending on whether they are incident or not, respectively. Thus the distance list of a line ℓ with respect to a point-set $\mathcal{S}$ is entirely determined by $\ell \cap \mathcal{S}$. Thus a semi-resolving set is a point-set which has a unique intersection with each line. It is clear that $\mathcal{S}$ resolves all lines that intersect it in at least two points. Therefore, $\mathcal{S}$ is a semi-resolving set iff $\mathcal{S}$ resolves its tangents and skew lines. Clearly, a double blocking set is a semi-resolving set.

PROPOSITION 4.1.3 ([F]). *A point-set $\mathcal{S}$ is a semi-resolving set for a projective plane if and only if the following hold:*

1. *there is at most one skew line to $\mathcal{S}$;*

2. *through every point of $\mathcal{S}$ there is at most one tangent line to $\mathcal{S}$.*

Proof. It is clear that $\mathcal{S}$ cannot have two or more skew lines. On the other hand, a unique skew line is clearly resolved. Let ℓ be a tangent to $\mathcal{S}$ with tangency point P (that is, $\ell \cap \mathcal{S} = \{P\}$). Then ℓ is resolved by $\mathcal{S}$ if and only if there are no other tangents to $\mathcal{S}$ through P. □

Let $\mu_S = \mu_S(\Pi_q)$ denote the size of the smallest semi-resolving set for Π_q. Blokhuis proved $\mu_S(\Pi_q) \geq 2q + \sqrt{2q}$ (unpublished); we are about to determine $\mu_S(\mathrm{PG}(2, q))$. Recall that $\tau_t = \tau_t(\Pi_q)$ denotes the size of the smallest t-fold blocking set in Π_q. The previous considerations immediately yield $\mu_S \leq \tau_2$. This and the first point of the next proposition were also pointed out by Bailey [7].

PROPOSITION 4.1.4 ([F]). *Let Π_q be an arbitrary projective plane. Then*

(i) $\mu_S \leq \tau_2 - 1$;

(ii) if $\mathcal{B}_1$ and $\mathcal{B}_2$ are disjoint blocking sets in Π_q, then $\mu_S \leq |\mathcal{B}_1| + |\mathcal{B}_2| - 2$;

(iii) in particular, if q is a square prime power, then $\mu_S(\mathrm{PG}(2, q)) \leq 2q + 2\sqrt{q}$; if $q = r^h$, $h \geq 3$ odd, r odd, then $\mu_S(\mathrm{PG}(2, q)) \leq 2(r^h + r^{h-1} + \ldots + r)$.

Proof. Let $\mathcal{B}$ a double blocking set, and let $P \in \mathcal{B}$. Then $\mathcal{S} = \mathcal{B} \setminus \{P\}$ is clearly a semi-resolving set [7], as there are no skew lines to $\mathcal{S}$, and through any point Q of $\mathcal{S}$ there is at most one tangent to $\mathcal{S}$, namely QP. By Proposition 4.1.3, this proves (i). To prove (ii), let $\mathcal{S} = (\mathcal{B}_1 \cup \mathcal{B}_2) \setminus \{P_1, P_2\}$ for some arbitrarily chosen $P_1 \in \mathcal{B}_1$, $P_2 \in \mathcal{B}_2$. Again, we check the requirements of Proposition 4.1.3. Clearly, there can be at most one skew line, namely P_1P_2. Take a point Q, say, from $\mathcal{B}_1 \setminus \{P_1\}$. As $\mathcal{B}_2$ intersects every line through Q, the only possible tangent line to $\mathcal{S}$ through Q is QP_2. Point (iii) follows immediately from point (ii) and Corollary 2.2.2. □

Proposition 4.1.5 ([F]). *Let $\mathcal{S}$ be a semi-resolving set for Π_q. Then $|\mathcal{S}| \geq 2q-1$.*

Proof. Suppose to the contrary that $|\mathcal{S}| \leq 2q-2$. If there is no tangent line to $\mathcal{S}$, take a point R outside $\mathcal{S}$. There is at most one skew line to $\mathcal{S}$ through R, the other q lines through R intersect $\mathcal{S}$ in at least two points, so $|\mathcal{S}| \geq 2q$, a contradiction.
Now suppose that there is a line ℓ tangent to $\mathcal{S}$. Count the other tangents of $\mathcal{S}$ through the points of ℓ. As there are at most $2q-2$ tangents to $\mathcal{S}$, there are at least two points in $\ell\setminus\mathcal{S}$ with at most one more tangent through them (besides ℓ). At least one of them, denote it by P, is not contained in the (possibly existing) skew line. At least $q-1$ lines through P are at least 2-secants to $\mathcal{S}$, one line is at least a 1-secant and ℓ is a tangent, so $|\mathcal{S}| \geq 2q$, a contradiction. □

From now on $\mathcal{S}$ denotes a semi-resolving set for PG$(2,q)$ of size $|\mathcal{S}| = 2q+\beta$, $\beta \in \mathbb{Z}$, $\beta \geq -1$. Almost every line intersects $\mathcal{S}$ in at least two points: at most $|\mathcal{S}|+1$ lines can be exceptional (that is, a (≤ 1)-secant). It would be natural to note how many exceptional lines are on a point P, yet we need a less straightforward number assigned to the points.

Definition 4.1.6. *Let $\mathcal{S}$ be a semi-resolving set. For a point P, let* $\mathrm{ind}_i(P)$ *be the number of i-secants to $\mathcal{S}$ through P. Let the* index *of P, denoted by* $\mathrm{ind}(P)$, *be* $2\,\mathrm{ind}_0(P) + \mathrm{ind}_1(P)$. *For the sake of simplicity, denote the index of the ideal point (m) by* $\mathrm{ind}(m)$ *instead of* $\mathrm{ind}((m))$.

Note that if $P \notin \mathcal{S}$, then $\mathrm{ind}(P) \leq 2$ (as there is at most one skew line through P); if $P \in \mathcal{S}$, then $\mathrm{ind}(P) \leq 1$ (as there are no skew lines and at most one tangent through P).

Proposition 4.1.7 ([F]). *Let $P \in \mathcal{P}\setminus\mathcal{S}$. Assume* $\mathrm{ind}(P) \leq q-2$, *and* $\beta \leq 2q-4$. *Let t be the number of tangents to $\mathcal{S}$ plus twice the number of skew lines to $\mathcal{S}$. Then*

$$\mathrm{ind}(P)^2 - (q-\beta)\,\mathrm{ind}(P) + t \geq 0, \tag{4.1}$$

and

$$\mathrm{ind}(P)^2 - (q-\beta)\,\mathrm{ind}(P) + 2q + \beta \geq 0. \tag{4.2}$$

Proof. As $\mathrm{ind}_0(P) + \mathrm{ind}_1(P) \leq \mathrm{ind}(P) \leq q-2$, there are at least three lines through P intersecting $\mathcal{S}$ in at least two points, and all other lines intersect $\mathcal{S}$

in at least one point except possibly the unique skew line. Among these three (≥ 2)-secants, there must be one intersecting $\mathcal{S}$ in $s \leq q-1$ points, otherwise $|\mathcal{S}| \geq 3q + q - 3 = 4q - 3$ would hold, contradicting $\beta \leq 2q - 4$.
Choose a coordinate system so that this s-secant line is the line at infinity ℓ_∞, $(\infty) \notin \mathcal{S}$ and $P \neq (\infty)$. This can be done as $s \leq q-1$. Let the set of the $|\mathcal{S}| - s$ affine points of $\mathcal{S}$ be $\{(x_i, y_i)\}_{i=1}^{|\mathcal{S}|-s}$. Denote by D the set of non-vertical directions that are outside $\mathcal{S}$, $D \subset \mathrm{GF}(q)$. As $(\infty) \notin \mathcal{S}$, $|D| = q - s$. Let

$$R(B, M) = \prod_{i=1}^{|\mathcal{S}|-s} (Mx_i + B - y_i) \in \mathrm{GF}(q)[B, M]$$

be the Rédei polynomial of $\mathcal{S} \cap \mathrm{AG}(2, q)$. If we substitute $M = m$ ($m \in \mathrm{GF}(q)$), then the multiplicity of the root b of the one-variable polynomial $R(m, B)$ is the number of affine points of $\mathcal{S}$ on the line $Y = mX + b$ (as seen in the proof of Theorem 2.1.1). Fix $m \in \mathrm{GF}(q)$, and recall that ℓ_∞ is a (≥ 2)-secant. Define k_m as $k_m = \deg\gcd(R(m, B), (B^q - B)^2)$. Thus k_m equals the number of single roots plus twice the number of roots of multiplicity at least two. If $m \in D$, then the number of lines with slope m that intersect $\mathcal{S} \cap \mathrm{AG}(2, q)$ in at least one point or in at least two points is $q - \mathrm{ind}_0(m)$ and $q - (\mathrm{ind}_0(m) + \mathrm{ind}_1(m))$, respectively, thus $k_m = q - \mathrm{ind}_0(m) + (q - \mathrm{ind}_0(m) - \mathrm{ind}_1(m)) = 2q - \mathrm{ind}(m)$.
We use the Szőnyi–Weiner Lemma (Result 1.1.3) with $u(B, M) = R(B, M)$ and $v(B, M) = (B^q - B)^2$. Note that the leading coefficient of both polynomials in B is one, so the Lemma applies. Let $P = (p)$ be our point on ℓ_∞ whose index shall be estimated. By the Szőnyi–Weiner Lemma,

$$\sum_{m \in D} (k_m - k_p) \leq \sum_{m \in \mathrm{GF}(q)} (k_m - k_p)^+ \leq (|\mathcal{S}| - s - k_p)(2q - k_p) = (\mathrm{ind}(P) + \beta - s)\,\mathrm{ind}(P).$$

On the other hand, let $\delta = \sum_{m \in D} \mathrm{ind}(m)$; that is, we count the tangents and the skew line intersecting ℓ_∞ in D with multiplicity one and two, respectively. Then $\sum_{m \in D}(k_m - k_p) = \sum_{m \in D}(\mathrm{ind}(P) - \mathrm{ind}(m)) = (q - s)\,\mathrm{ind}(P) - \delta$. Combined with the previous inequality we get

$$\mathrm{ind}(P)^2 - (q - \beta)\,\mathrm{ind}(P) + \delta \geq 0.$$

As $\delta \leq t$, we obtain inequality (4.1). Furthermore, as the (possibly not existing) skew line (counted with multiplicity two) may have a slope in D, and the (possibly not existing) tangents through the s ($s \geq 2$) points in $\ell_\infty \cap \mathcal{S}$ are not counted in δ, we have $\delta \leq |\mathcal{S}| - s + 2 \leq |\mathcal{S}| = 2q + \beta$. This gives inequality (4.2). $\square$

Proposition 4.1.8 ([F]). *Suppose $\beta \leq q/4 - 5/2$. Let $P \notin \mathcal{S}$. Then* $\mathrm{ind}(P) \leq 2$ *or* $\mathrm{ind}(P) \geq q - \beta - 2$.

Proof. Suppose that $P \notin \mathcal{S}$ and $\mathrm{ind}(P) \leq q-2$ (in order to use inequality (4.2) in Proposition 4.1.7). Substituting $\mathrm{ind}(P) = 3$ or $\mathrm{ind}(P) = q-\beta-3$ into (4.2), we get $\beta \geq (q-9)/4$, a contradiction. Thus either $\mathrm{ind}(P) \leq 2$, or $\mathrm{ind}(P) \geq q-\beta-2$. $\square$

Hence, if $\beta \leq q/4 - 5/2$, we may call the index of a point large or small, according to the two possibilities above.

Proposition 4.1.9 ([F]). *Assume $\beta \leq q/4 - 5/2$ and $q \geq 4$. Then on every tangent to $\mathcal{S}$ there is at least one point with large index, and on the skew line, if exists, there are at least two points with large index.*

Proof. Let ℓ be a skew line. A tangent line intersects ℓ in a point with index at least three, hence in a point with large index. If there were at most one point with large index on ℓ, then there would be at most q tangents to $\mathcal{S}$, whence the parameter t in Proposition 4.1.7 would be at most $q + 2$. A point P on ℓ with small index has index two, while by inequality (4.1) we have $\mathrm{ind}(P)^2 - (q - \beta)\,\mathrm{ind}(P) + q + 2 = 2\beta + 6 - q \geq 0$, in contradiction with $\beta \leq q/4 - 5/2$ under $q \geq 4$.

Suppose that ℓ is tangent to $\mathcal{S}$. Suppose that all indices on ℓ are at most two. Then there is no skew line to $\mathcal{S}$ as the intersection point would have index at least three. Then we have $t \leq 1 + q$. If there is a point $P \in \ell \setminus \mathcal{S}$ with index two, (4.1) gives $4 - 2(q - \beta) + q + 1 = \beta + 5 - q \geq 0$, a contradiction. If all points on ℓ have index one, then $t = 1$, and (4.1) yields $2 - q + \beta \geq 0$, again a contradiction. $\square$

Theorem 4.1.10 ([F]). *Let $\mathcal{S}$ be a semi-resolving set for* PG$(2, q)$, $q \geq 4$. *If $|\mathcal{S}| < 2q + q/4 - 3$, then one can add at most two points to $\mathcal{S}$ to obtain a double blocking set.*

Proof. In other words, the upper bound on $\mathcal{S}$ says $\beta < q/4 - 3$. As Proposition 4.1.8 applies, indices are either small or large. Recall that the points with large index are not in $\mathcal{S}$. Proposition 4.1.9 yields that by adding the points with large index to $\mathcal{S}$ we obtain a double blocking set. Therefore, we only have to show that there are at most two points with large index. Suppose to the contrary, and let P_1, P_2 and P_3 be three points with large index. The number of tangent lines through P_i ($i = 1, 2, 3$) is at least $q-\beta-4$ or $q-\beta-2$, according to whether P_i is incident with a skew line or not, respectively. If P_1, P_2 and P_3 are collinear, we find at least $3(q-\beta-4)$ tangents to $\mathcal{S}$. If they are in general position, at most two of them are incident with a skew line, so again we find at least $3(q-\beta-4)$ tangents to $\mathcal{S}$. Thus $3(q-\beta-4) \leq |\mathcal{S}| = 2q+\beta$, in contradiction with $\beta < q/4-3$. □

This immediately yields the following theorem.

THEOREM 4.1.11 ([F]). *Let $\mathcal{S}$ be a semi-resolving set for* PG$(2, q)$*, $q \geq 4$. Then $|\mathcal{S}| \geq \min\{9q/4-3, \tau_2(\mathrm{PG}(2,q))-2\}$.*

Compared with our recent knowledge on τ_2, we obtain the following. Recall that $\mu_S(\mathrm{PG}(2,q))$ is the size of the smallest semi-resolving set for PG$(2, q)$.

COROLLARY 4.1.12 ([F]).

(i) If $q \geq 121$ is a square prime power, then $\mu_S(\mathrm{PG}(2,q)) = 2q+2\sqrt{q}$. Moreover, if $q > 256$, then semi-resolving sets attaining equality are the union of two punctured, disjoint Baer subplanes (cf. Proposition 4.1.4 (iii)).

(ii) If $q = r^h$, $h \geq 3$ odd, and $r \geq 11$ is an odd prime power (possibly a prime), then $\tau_2 - 2 \leq \mu_S(\mathrm{PG}(2,q)) \leq \tau_2 - 1$.

Proof. Regarding (i), Result 1.5.7 yields $\tau_2(\mathrm{PG}(2,q)) = 2q+2\sqrt{q}+2$ for $q \geq 9$ square, hence $\tau_2 - 2 \leq 2q+q/4-3$ is equivalent to $2\sqrt{q}+3 \leq q/4$, which holds if $q \geq 121$. Thus Theorem 4.1.11 gives $\mu_S \geq \tau_2 - 2$, while Proposition 4.1.4 (ii) shows that equality holds. Result 1.5.8 yields that in PG$(2, q)$, $q > 256$, any double blocking set of size $2(q+\sqrt{q}+1)$ is the union of two disjoint Baer subplanes. The two missing points cannot lie in the same Baer subplane, as otherwise we could easily find a point in the other Baer-subplane with two tangents.

As for (ii), Theorem 2.2.1 gives $\tau_2 - 2 \leq 2q+2(q-1)/(r-1)-2$, which is not larger than $2q+q/4-3$ if and only if $q-1 \leq (r-1)(q-4)/8$. By $r \geq 11$ and $q \geq r^3$, this inequality is satisfied. Thus Theorem 4.1.11 gives the lower bound. The upper bound comes from Proposition 4.1.4 (i). □

We remark that for small values of q, there are semi-resolving sets smaller than $\tau_2 - 2$. Three points in general position show $\tau_2(\mathrm{PG}(2,2)) = 3$. A vertexless triangle (the union of the point-set of three lines in general position without their three intersection points) is easily seen to be a semi-resolving set of size $3q-3$ for $q \geq 3$. If $q \geq 4$, we may remove one more (arbitrary) point to obtain a semi-resolving set of size $3q-4$. (In fact, there are no smaller semi-resolving sets than the previous ones for $q = 2, 3, 4$.) On the other hand, $\tau_2(\mathrm{PG}(2,q)) = 3q$ for $q = 2, 3, 4, 5, 7, 8$ (mentioned in [13]; this result is due to various authors).

4.2 A note on blocking semiovals

Finally, let us mention an immediate consequence of Theorem 4.1.10 on the size of blocking semiovals. The connection between blocking semiovals and semi-resolving sets was pointed out by Csajbók [29]. For more information on semiovals, we refer to [54].

DEFINITION 4.2.1. *A point-set $\mathcal{S}$ in a finite projective plane is a* semioval*, if for all $P \in \mathcal{S}$, there is exactly one tangent to $\mathcal{S}$ through P. A semioval $\mathcal{S}$ is a* blocking semioval*, if there are no skew lines to $\mathcal{S}$.*

Lower bounds on the size of blocking semiovals are of interest. Up to our knowledge, the following is the best bound known.

RESULT 4.2.2 (Dover [34]). *Let $\mathcal{S}$ be a blocking semioval in an arbitrary projective plane of order q. If $q \geq 7$, then $|\mathcal{S}| \geq 2q+2$. If $q \geq 3$ and there is a line intersecting $\mathcal{S}$ in $q-k$ points, $1 \leq k \leq q-1$, then $|\mathcal{S}| \geq 3q - 2q/(k+2) - k$.*

COROLLARY 4.2.3 ([F]). *Let $\mathcal{S}$ be a blocking semioval in $\mathrm{PG}(2,q)$, $q \geq 4$. Then $|\mathcal{S}| \geq 9q/4 - 3$.*

Proof. By Proposition 4.1.3, $\mathcal{S}$ is clearly a semi-resolving set. Suppose to the contrary that $|\mathcal{S}| < 9q/4 - 3$. Then by Theorem 4.1.10, we find two points, P and Q, such that $\mathcal{S} \cup \{P, Q\}$ is a double blocking set, that is, P and Q block all the $|\mathcal{S}|$ tangents to $\mathcal{S}$. On the other hand, $|\mathcal{S}| \geq \tau_2 - 2 > 2q+1$ (here we use $q \geq 4$ and $\tau_2 = 3q$ for $q \leq 8$, $\tau_2 \geq 2q + 2\sqrt{q} + 2$ for $q \geq 9$.) Hence $\mathcal{S}$ has more than $2q+1$ tangents. However, P and Q can block at most $2q+1$ of them, a contradiction. □

Note that Dover's result is better than Corollary 4.2.3 if there is a line intersecting the blocking semioval in more than $q/4$ points (roughly).

4.3 Remarks

Note that if we knew that the double blocking sets of size $\tau_2(\mathrm{PG}(2,q))$ in $\mathrm{PG}(2,q)$ are the union of two disjoint blocking sets, then we would have $\mu_S(\mathrm{PG}(2,q)) = \tau_2(\mathrm{PG}(2,q)) - 2$ in Corollary 4.1.12 (ii).

One motivation to study semi-resolving sets for projective planes was to construct resolving sets; clearly, if we take the union of two semi-resolving sets, one of which resolves the lines, the other of which resolves the points, we obtain a resolving set for the whole projective plane. Bailey [7] calls such resolving sets split resolving sets. By Theorem 4.1.11 we have that the smallest split resolving set in PG$(2,q)$, $q \geq 4$, has at least $\min\{9q/2-6, 2\tau_2-4\}$ points. Regarding (non-split) resolving sets, in [F] we prove that the smallest resolving set for Π_q, $q \geq 23$, has exactly $4q-4$ points, which is definitely smaller than the size of the smallest split resolving set.

Chapter 5

The upper chromatic number of $\mathrm{PG}(2, q)$

5.1 Introduction

The almost classical area of finite geometries and a very young area, the coloring theory of mixed hypergraphs are combined in this chapter. For general information on the latter, we refer to [75]. We discuss only a particular problem of the coloring theory of mixed hypergraphs, so we do not give the general definitions. The chapter is based on [B].

The upper chromatic number of a hypergraph $\mathcal{H}$ is the maximum number $\mathrm{UCN}(\mathcal{H})$ of colors with which one can color the points of $\mathcal{H}$ without creating a rainbow hyperedge (a hyperedge is rainbow, if no two of its points have the same color). This is the counterpart of the traditional chromatic number in some sense: there we color the points with as few colors as possible while avoiding monochromatic hyperedges. Note that the upper chromatic number of an ordinary graph is the number of its connected components.

Let $\Pi_q = (\mathcal{P}, \mathcal{L})$ denote a finite projective plane of order q. Considering Π_q as a hypergraph, we wish to determine $\mathrm{UCN}(\Pi_q)$; that is, we wish to color the points of Π_q with as many colors as possible without creating a line whose points have pairwise distinct colors. Throughout this chapter, let $v = |\mathcal{P}| = q^2 + q + 1$.

Definition 5.1.1. *We say that a coloring of the points of a finite projective plane* Π *is* proper*, if every line contains at least two points of the same color. The* upper chromatic number of Π*, in notation* $\mathrm{UCN}(\Pi)$*, is the maximum number of colors one may use in a proper coloring.*

Note that it if we merge color classes of a proper coloring (i.e., replace two color classes C_i and C_j by $C_i \cup C_j$), then the resulting coloring is also proper.

In [6] the following general bound is given on the upper chromatic number for any projective plane, as a function of the order, and thus a ten-year-old open problem is solved in the coloring theory of mixed hypergraphs.

RESULT 5.1.2 (Bacsó–Tuza [6]). *As $q \to \infty$, any projective plane Π_q of order q satisfies*

$$\mathrm{UCN}(\Pi_q) \leq q^2 - q - \sqrt{q}/2 + o(\sqrt{q}).$$

If $\mathcal{B}$ is a double blocking set in Π_q, coloring the points of $\mathcal{B}$ with one color and all points outside $\mathcal{B}$ with mutually distinct colors, one gets a proper coloring of Π_q with $v - |\mathcal{B}| + 1$ colors. To achieve the best possible out of this idea, one should take $\mathcal{B}$ a smallest double blocking set. Recall that $\tau_2 = \tau_2(\Pi_q)$ denotes the size of the smallest double blocking set in Π_q. We have obtained

PROPOSITION 5.1.3.

$$\mathrm{UCN}(\Pi_q)) \geq v - \tau_2 + 1.$$

DEFINITION 5.1.4. *A coloring of Π_q is* trivial*, if it contains a monochromatic double blocking set of size τ_2, and every other color class consists of one single point. A* nontrivial *coloring is a proper coloring that is not trivial.*

Let us cite a more general result of [6]. Let $\tau_2(\Pi_q) = 2(q+1) + c(\Pi_q)$. Note that Proposition 5.1.3 claims $\mathrm{UCN}(\Pi_q) \geq q^2 - q - c(\Pi_q)$.

RESULT 5.1.5 (Bacsó–Tuza [6]). *Let Π_q be an arbitrary finite projective plane of order q. Then*

$$\mathrm{UCN}(\Pi_q) \leq q^2 - q - \frac{c(\Pi_q)}{2} + o(\sqrt{q}).$$

If $c(\Pi_q)$ is not too small (roughly, $c(\Pi_q) > 24q^{2/3}$), we improve this result combinatorially. Moreover, we show that (under some technical conditions) the lower bound of Proposition 5.1.3 is sharp in $\mathrm{PG}(2,q)$ if q is not a prime, and it is almost sharp if q is a prime and τ_2 is small enough. In the proof we use algebraic results as well, and we also rely on Corollary 2.2.2, the upper bound on τ_2. The precise results are the following.

THEOREM 5.1.6 ([B]). *Let Π_q be an arbitrary projective plane of order $q \geq 8$, and let $\tau_2(\Pi_q) = 2(q+1) + c(\Pi_q)$. Then*

$$\mathrm{UCN}(\Pi_q) < q^2 - q - \frac{2c(\Pi_q)}{3} + 4q^{2/3}.$$

THEOREM 5.1.7 ([B]). *Let* $v = q^2 + q + 1$. *Suppose that* $\tau_2(\mathrm{PG}(2,q)) \leq c_0 q - 8$, $c_0 < 8/3$, *and let* $q \geq \max\{(6c_0 - 11)/(8 - 3c_0), 15\}$. *Then*

$$\mathrm{UCN}(\mathrm{PG}(2,q)) < v - \tau_2 + \frac{c_0}{3 - c_0}.$$

Note that $\frac{c_0}{3-c_0} < 8$.

THEOREM 5.1.8 ([B]). *Let* $v = q^2 + q + 1$, $q = p^h$, *p prime, and suppose that* $q > 256$ *is a square, or* $p \geq 29$ *and* $h \geq 3$ *odd. Then* $\mathrm{UCN}(\mathrm{PG}(2,q)) = v - \tau_2 + 1$, *and equality is reached only by trivial colorings.*

5.2 Proof of the results

Let Π_q be a finite projective plane of order q. Let $\mathcal{C} = \{C_1, \ldots, C_m\}$ be a proper coloring, where the point-set of Π_q is partitioned by the color classes C_i, $i = 1, \ldots, m = m(\mathcal{C})$. We may assume that $|C_1| \geq |C_2| \geq \ldots |C_n| \geq 2$, $|C_{n+1}| = \ldots = |C_m| = 1$ for some appropriate $n = n(\mathcal{C})$. A color class of size exactly d will be called a *d-class*. We say that *a color class* C_i *colors a line* ℓ, if $|\ell \cap C_i| \geq 2$. Let $\mathcal{B} = \mathcal{B}(\mathcal{C}) = \cup_{i=1}^{n} C_i$. As every line must be colored, $\mathcal{B}$ is a double blocking set. We always assume that a proper coloring $\mathcal{C}$ of the plane is given.

With the above notation, $\mathcal{C}$ uses $v - |\mathcal{B}| + n$ colors, while a trivial coloring has $v - |\tau_2| + 1$ colors. Thus to achieve this bound, we need to have $n \geq |\mathcal{B}| - \tau_2 + 1$. We define the parameter $e = e(\mathcal{C})$, standing for excess, which measures how much our coloring is better than a trivial one.

DEFINITION 5.2.1.

$$e := n - |\mathcal{B}| + \tau_2 - 1.$$

To avoid colorings that are worse than the trivial ones, we will usually suppose that $e \geq 0$ (equivalently, $n \geq |\mathcal{B}| - \tau_2 + 1$). First we formulate a straightforward observation.

PROPOSITION 5.2.2 ([B]). *If* $\mathcal{C}$ *is a nontrivial proper coloring with* $e(\mathcal{C}) \geq 0$, *then* $\mathcal{C}$ *does not contain a monochromatic double blocking set.*

Proof. Suppose to the contrary that $\mathcal{C}$ contains a monochromatic double blocking set $\mathcal{S}$. Then $v - \tau_2 + 1 \leq m(\mathcal{C}) \leq v - |\mathcal{S}| + 1 \leq v - \tau_2 + 1$, so $|\mathcal{S}| = \tau_2$ and all other color classes are 1-classes, thus $\mathcal{C}$ is trivial, a contradiction. □

The following lemma shows that we can eliminate all but possibly one 2-classes.

LEMMA 5.2.3 ([B]). *Let $\mathcal{C}$ be proper coloring of Π_q. Then there is another proper coloring $\mathcal{C}'$ with the same number of colors such that there is at most one 2-class in $\mathcal{C}'$. If there is a 2-class in $\mathcal{C}'$, then its points are essential with respect to $\mathcal{B}(\mathcal{C}')$. Moreover, if $\Pi_q = \mathrm{PG}(2, q)$, $\tau_2 < 3q$, and $\mathcal{C}$ is nontrivial, then $\mathcal{C}'$ is also nontrivial.*

Proof. We construct $\mathcal{C}'$ step by step from $\mathcal{C}$; the notation always regard to the coloring obtained at the last step. Consider a 2-class $C_i = \{P, Q\}$. Then it colors only one line, namely PQ. If PQ intersects $\mathcal{B}$ in a point R, $R \in C_j$ $(i \neq j)$, then remove P from C_i and put it into C_j. As $PQ = PR$ is now colored by the class C_j, we obtain a proper coloring. Note that C_j originally had at least two points, so we did not create a new 2-class. Repeat this operation until every 2-class colors a line that is a two-secant to $\mathcal{B}$. Now suppose that there are two 2-classes $C_i = \{P_1, P_2\}$ and $C_j = \{Q_1, Q_2\}$ $(i \neq j)$ such that P_1P_2 and Q_1Q_2 are two-secants to $\mathcal{B}$. Then $R = P_1P_2 \cap Q_1Q_2$ is not in $\mathcal{B}$, so $\{R\} = C_h$ is a singleton color class. Remove P_1 from C_i and Q_1 from C_j, and put both into C_h. Again it is clear that we obtain a proper coloring, and we do not create new 2-classes. Repeating this operation we can decrease the number of 2-classes to at most one. If a 2-class $\{P, Q\}$ remains uneliminated, then PQ is a two-secant, hence P and Q are essential. Thus the first part of the lemma is proved.

Now suppose to the contrary that $\Pi_q = \mathrm{PG}(2, q)$, the original coloring $\mathcal{C}$ is nontrivial, but we obtain a trivial coloring $\mathcal{C}'$. Then at the last step we eliminated every color class of size two, and we created a monochromatic double blocking set of size τ_2. We must have used the first operation at this step (in the second operation no color classes of size more than three are involved), so we put a point from $C_i = \{P, Q\}$ to C_j. As both points of C_i could be used, $C_j \cup \{P\}$ and $C_j \cup \{Q\}$ are both double blocking sets of size τ_2. Hence $C_i \cup C_j$ is a double blocking set of size $\tau_2 + 1 \leq 3q$ which contains two minimal double blocking sets, in contradiction with Corollary 2.1.3. □

By the above lemma, from now on we may rely on the assumption that there is at most one 2-class.

PROPOSITION 5.2.4 ([B]). *Suppose that $\mathcal{B}$ contains at most one 2-class and $e \geq 0$. Then $n \leq \tau_2/2$.*

Proof. As there is at most one 2-class and all other color classes in $\mathcal{B}$ have at least three points, we have $n \leq 1 + (|\mathcal{B}| - 2)/3$. By $e \geq 0$, $|\mathcal{B}| - \tau_2 + 1 \leq n \leq 1+(|\mathcal{B}|-2)/3$, hence $|\mathcal{B}| \leq 3\tau_2/2-1$. Thus we have $n \leq 1+(|\mathcal{B}|-2)/3 \leq \tau_2/2$. □

Now let us recall and prove our combinatorial result on $\mathrm{UCN}(\Pi_q)$.

THEOREM 5.1.6 ([B]). *Let Π_q be an arbitrary projective plane of order $q \geq 8$, and let $\tau_2(\Pi_q) = 2(q+1) + c(\Pi_q)$. Then*

$$\mathrm{UCN}(\Pi_q) < q^2 - q - \frac{2c(\Pi_q)}{3} + 4q^{2/3}.$$

Proof. Take a proper coloring $\mathcal{C}$. We will estimate the number of colors in $\mathcal{C}$. We may assume that $e(\mathcal{C}) \geq 0$ (otherwise the statement is trivial), moreover, by Lemma 5.2.3, we may also suppose that there is at most one 2-class in $\mathcal{C}$. Set $\varepsilon = 4/\sqrt[3]{q}$, and let h denote the number of color classes with at least $K = 6/\varepsilon$ elements (obviously, $K \geq 3$). Let $\mathcal{S} = \cup_{i=1}^{h} C_i$.

First suppose $|\mathcal{S}| \leq 2(1-\varepsilon)q$. Let $P \notin \mathcal{S}$. As the number of lines through P that intersect $\mathcal{S}$ in at least two points is at most $|\mathcal{S}|/2$, there are at least εq lines through P that intersect $\mathcal{S}$ in at most one point. Hence the total number of such lines is at least $(q^2+q+1-|\mathcal{S}|)\varepsilon q/(q+1) > \varepsilon q(q-2)$. On the other hand, color classes of size less than K can color at most $(n-h)\binom{K}{2} \leq (n-h)K^2/2$ lines, thus $(n-h)K^2 \geq 2\varepsilon q(q-2)$ must hold. Therefore, by Proposition 5.2.4, $3q/2 \geq \tau_2/2 \geq n \geq 2\varepsilon q(q-2)/K^2 = \varepsilon^3 q(q-2)/18$ holds. As $\varepsilon = 4/\sqrt[3]{q}$, this yields $27 \geq 64(q-2)/q$, in contradiction with $q \geq 8$.

Thus $|\mathcal{S}| > 2(1-\varepsilon)q$ may be supposed. As all but one color classes in $\mathcal{B}$ have at least three points, for the number n of colors used in $\mathcal{B}$, $n \leq |\mathcal{S}|/K + (|\mathcal{B}| - |\mathcal{S}|)/3 + 1$ holds. Since $K \geq 3$, by substituting $|\mathcal{S}| = 2(1-\varepsilon)q$ we increase the right-hand side, so $n \leq 2(1-\varepsilon)q/K + (|\mathcal{B}| - 2(1-\varepsilon)q)/3 + 1$. Using $|\mathcal{B}| \geq \tau_2$, for the total number $m = n + q^2 + q + 1 - |\mathcal{B}|$ of colors we get $m \leq q^2 + q + 2 - 2\tau_2/3 - 2(1-\varepsilon)q(1/3 - 1/K)$. By $\tau_2 = 2q + c(\Pi_q) + 2$, we obtain that

$$n \leq q^2 - q - \frac{2}{3}c(\Pi_q) + \frac{2\varepsilon}{3}q + \frac{2(1-\varepsilon)}{K}q.$$

As $K = 6/\varepsilon$, we get

$$\mathrm{UCN}(\Pi_q) < q^2 - q - \frac{2}{3}c(\Pi_q) + \varepsilon q.$$

□

Attention. From now on, we only consider proper colorings of Desarguesian projective planes; that is, we assume $\Pi_q = \mathrm{PG}(2,q)$, $q = p^h$, p prime.

In the sequel, we show that if τ_2 is small, then a nontrivial coloring can not have $e \geq 0$. We handle three cases separately, depending on $|\mathcal{B}|$ being at least

$3q-\alpha$, between $\tau_2+\xi$ and $3q-\alpha$, or at most $\tau_2+\xi$, where α and ξ are small constants. In the next proposition we use the well-known fact that if f is a convex function and $x \le y$, then $f(x+\varepsilon)+f(y-\varepsilon) \ge f(x)+f(y)$ for arbitrary $\varepsilon > 0$. Therefore if the sum of the input $x_1, \dots, x_n$ is fixed and the x_is are bounded from below, then $\sum_{i=1}^n f(x_i)$ takes its maximum value iff all but one of the x_is meet their lower bound (so the input is spread). However, the function we are about to consider is not entirely convex, so at some point we cannot modify the input by an arbitrarily small ε, but only with a large enough value to see that the maximum value is taken if and only if the input is spread.

PROPOSITION 5.2.5 ([B]). *Suppose that there is at most one 2-class in $\mathcal{B}$. Let $|\mathcal{B}| \ge 3q-\alpha$ for some integer α, $0 \le \alpha \le q-5$, and suppose $\tau_2 \le c_0q-\beta$, where $c_0 < 8/3$ and $\beta = (2\alpha+4)/3$. Assume $q \ge q(c_0) = (6c_0-11)/(8-3c_0)$. Then $e < 0$.*

Proof. Suppose to the contrary that $e \ge 0$. Then $n \ge |\mathcal{B}| - \tau_2 + 1 \ge 3q - \alpha - 8q/3 + \beta = (q-\alpha+4)/3 \ge 3$.

Denote by $\ell(C_i)$ the number of lines colored by C_i, $i = 1, \dots, n$. It is straightforward that $\ell(C_i) \le \binom{|C_i|}{2}$. On the other hand, counting selected point-line pairs, we get

$$2\ell(C_i) \le |\{(P,e)\colon P \in e \cap C_i, |e \cap C_i| \ge 2\}| \le (q+1)|C_i|,$$

whence

$$\ell(C_i) \le \frac{q+1}{2}|C_i|$$

follows. Therefore $\ell(C_i) \le \min\left\{\binom{|C_i|}{2}, \frac{q+1}{2}|C_i|\right\} =: f(|C_i|)$. Note that the second upper bound is smaller than or equal to the first one iff $|C_i| \ge q+2$. As every line must be colored by at least one color class, we have

$$q^2+q+1 \le \sum_{i=1}^n \ell(C_i) \le \sum_{i=1}^n f(|C_i|),$$

where $\sum_{i=1}^n |C_i| = |\mathcal{B}|$ is fixed. We will give an upper bound on the right-hand-side. Extend the function f to $\mathbb{R}$. Then f is increasing and convex on $[2, q+2]$, linear on $[q+2, \infty)$, but it is not convex on $[2, \infty)$. Recall that $|C_1| \ge \ldots \ge |C_n| \ge 2$, $n = |\mathcal{B}| - \tau_2 + 1 + e \ge |\mathcal{B}| - \tau_2 + 1$, and that there is at most one 2-class in $\mathcal{B}$. Note that $3\tau_2 - 2|\mathcal{B}| \le 3c_0q - 3\beta - 6q + 2\alpha = (3c_0-6)q - 4 < 2q - 4$.

We claim that $|C_2| \le q-1$. If $|C_1| \ge q$, then by $n \ge |\mathcal{B}| - \tau_2 + 1$, we have $|C_2| \le |\mathcal{B}| - q - 2 - 3(n-3) \le 3\tau_2 - 2|\mathcal{B}| - q + 4 < q$. On the other hand, if

$|C_1| \le q-1$, then $|C_2| \le |C_1|$ also implies $|C_2| \le q-1$. As there is at most one 2-class, $|C_2| \ge 3$ follows from $n \ge 3$. As $2 \le |C_i| \le q-1$ for all $2 \le i \le n$ and f is convex on this interval, $\sum_{i=2}^{n} f(|C_i|)$ achieves its largest possible value if $|C_n| = 2$, $|C_{n-1}| = \ldots = |C_3| = 3$, and $|C_2| = |\mathcal{B}| - |C_1| - \sum_{i=3}^{n} |C_i|$. By substituting these values,

$$\sum_{i=1}^{n} f(|C_i|) \le \frac{q+1}{2}|C_1| + \sum_{i=2}^{n} \binom{|C_i|}{2} \le \frac{q+1}{2}|C_1| + \binom{|C_2|}{2} + (n-3)\binom{3}{2} + \binom{2}{2}.$$

Now we claim that

$$\frac{q+1}{2}|C_1| + \binom{|C_2|}{2} \le \frac{q+1}{2}(|C_1| + |C_2| - 3) + \binom{3}{2}, \tag{5.1}$$

which is equivalent to $|C_2|^2 - (q+2)|C_2| + 3q - 3 \le 0$. It is easy to see that this latter inequality holds for $|C_2| \in [3, q-1]$, so we may use (5.1). Recall $n \le \tau_2/2$ (Proposition 5.2.4) and $3\tau_2 - 2|\mathcal{B}| \le (3c_0-6)q-4$. As $|C_1|+|C_2| \le |\mathcal{B}|-2-3(n-3)$,

$$q^2 + q + 1 \le \sum_{i=1}^{n} f(|C_i|) \le \frac{q+1}{2}(|\mathcal{B}| + 4 - 3n) + 3(n-2) + 2 \le$$

$$\frac{q+1}{2}(|\mathcal{B}| + 4 - 3(|\mathcal{B}| - \tau_2 + 1)) + 3(\tau_2/2 - 2) + 2 \le \frac{q+1}{2}(3\tau_2 - 2|\mathcal{B}| + 1) + \frac{3}{2}\tau_2 - 4.$$

For aesthetic reasons, we continue with a strict inequality. The last value is less than

$$\frac{q+1}{2}((3c_0-6)q-3) + \frac{3}{2}c_0 q + \frac{5}{2} = \left(\frac{3c_0}{2} - 3\right)q^2 + \left(3c_0 - \frac{9}{2}\right)q + 1.$$

This is equivalent to $(8-3c_0)q^2 - (6c_0-11)q < 0$, hence, as $c_0 < 8/3$, we obtain $q < (6c_0-11)/(8-3c_0)$, a contradiction. □

Next we investigate the case when $\mathcal{B}$ is of medium size. We show that in this case there are some large color classes, which bounds the total number of color classes. Note that the next proposition does not use any assumptions on $|\mathcal{B}|$, however, it is meaningful only if $|\mathcal{B}| < 3q$.

PROPOSITION 5.2.6 ([B]). *Every color class containing an essential point of $\mathcal{B}$ has at least $(3q - |\mathcal{B}| + 2)$ points.*

Proof. Let $P \in \mathcal{B}$ be an essential point. Let $|\mathcal{B}| = 2(q+1)+k$. Then by Theorem 2.1.1 there are $(q-1-k) = 3q - |\mathcal{B}| + 1$ two-secants through P. The points of a two-secant must have the same color. □

REMARK 5.2.7. *Proposition 5.2.6 shows that if* $|\mathcal{B}| < 3q$, *then color classes containing an essential point have at least three points. Thus by Lemma 5.2.3, every 2-class can be eliminated.*

PROPOSITION 5.2.8 ([B]). *Assume that* $|\mathcal{B}| < 3q$, *and suppose that there are no color classes of size two. Then*

$$\left(\frac{2}{3}(|\mathcal{B}| - \tau_2) + e + 1\right)(3q - |\mathcal{B}| + 2) \leq \tau_2. \tag{5.2}$$

Proof. Consider a minimal double blocking set $\mathcal{B}' \subset \mathcal{B}$. Corollary 2.1.3 yields that $\mathcal{B}'$ consists precisely of the set of essential points of $\mathcal{B}$. Thus color classes intersecting $\mathcal{B}'$ must have at least $3q - |\mathcal{B}| + 2$ points (Proposition 5.2.6), while color classes disjoint from $\mathcal{B}'$ contain at least three points. Thus the total number of color classes in $\mathcal{B}$,

$$n \leq \frac{|\mathcal{B}'|}{3q - |\mathcal{B}| + 2} + \frac{|\mathcal{B}| - |\mathcal{B}'|}{3}.$$

Recall $n = |\mathcal{B}| - \tau_2 + 1 + e$ (Definition 5.2.1). As $|\mathcal{B}'| \geq \tau_2$ and $3q - |\mathcal{B}| + 2 \geq 3$, we obtain

$$|\mathcal{B}| - \tau_2 + 1 + e \leq \frac{\tau_2}{3q - |\mathcal{B}| + 2} + \frac{|\mathcal{B}| - \tau_2}{3},$$

which is clearly equivalent to the formula stated. □

Now we recall and prove Theorem 5.1.7.

THEOREM 5.1.7 ([B]). *Suppose that* $\tau_2(\mathrm{PG}(2,q)) \leq c_0 q - 8$, $2 \leq c_0 < 8/3$, *and let* $q \geq \max\{(6c_0 - 11)/(8 - 3c_0), 15\}$. *Then*

$$\mathrm{UCN}(\mathrm{PG}(2,q)) < v - \tau_2 + \frac{c_0}{3 - c_0}.$$

Proof. Let $\mathcal{C}$ be a proper coloring of $v - \tau_2 + 1 + e$ colors. Suppose to the contrary that $e \geq c_0/(3 - c_0) - 1$. As $c_0 \geq 2$, this yields $e \geq 1$. By Lemma 5.2.3, we may assume that there is at most one 2-class in $\mathcal{C}$.

Suppose that $|\mathcal{B}| \geq 3q - 10$. By the assumptions of the present theorem, the assumptions of Proposition 5.2.5 are also satisfied for $\alpha = 10$. Then we get $e < 0$, a contradiction.

Thus we may assume $|\mathcal{B}| \leq 3q - 11$. Then by Remark 5.2.7, we may use Proposition 5.2.8 to obtain

$$\left(\frac{2(|\mathcal{B}| - \tau_2)}{3} + e + 1\right)(3q - |\mathcal{B}| + 2) < c_0 q.$$

We will show that this can not hold. Note that the expression on the left-hand-side is concave in $|\mathcal{B}|$, so it is enough to verify that we get a contradiction for the extremal values $|\mathcal{B}| = \tau_2$ and $|\mathcal{B}| = 3q - 11$. By substituting $|\mathcal{B}| = \tau_2 < c_0 q$, we easily obtain $(e+1)(3q - c_0 q) < c_0 q$, thus $e < c_0/(3 - c_0) - 1$, a contradiction. Substituting $|\mathcal{B}| = 3q - 11$, using $\tau_2 \le c_0 q - 8$ and $e \ge 1$, we get

$$\left(\frac{2(3q - 11 - c_0 q + 8)}{3} + 2\right) \cdot 13 < c_0 q,$$

which results in $84 < 29c_0 < 80$, a contradiction. Thus $e < c_0/(c_0 - 3) - 1$. As $c_0 < 8/3$, we have $e < 7$, hence $e \le 6$ also follows. □

To obtain tight results, we need to investigate the case when $|\mathcal{B}|$ is close to τ_2. If such a double blocking set is the union of two disjoint blocking sets (e.g., in $\mathrm{PG}(2, q)$, if q is a square), we easily find two large color classes, so $|\mathcal{B}|$ must be big.

PROPOSITION 5.2.9 ([B]). *Let $\mathcal{C}$ be a nontrivial proper coloring, and suppose that $\mathcal{B}$ contains the union of two disjoint (1-fold) blocking sets, $\mathcal{B}_1$ and $\mathcal{B}_2$, such that $\mathcal{B}_1 \cup \mathcal{B}_2$ is a minimal double blocking set. Then $|\mathcal{B}| > 12q/5$.*

Proof. We may assume $|\mathcal{B}| \le 3q$. By Corollary 2.1.3, $\mathcal{B}_1 \cup \mathcal{B}_2$ is precisely the set of essential points of $\mathcal{B}$. As $\mathcal{C}$ is nontrivial, Proposition 5.2.2 assures that at least two colors, say, red and green, are used to color the points of $\mathcal{B}_1 \cup \mathcal{B}_2$. We may assume that there is a red point P in $\mathcal{B}_1$. Then by Theorem 2.1.1, there are at least $3q - |\mathcal{B}| + 1$ distinct 2-secants to $\mathcal{B}$ through P. As $\mathcal{B}_2$ is a blocking set, each of these lines intersects $\mathcal{B}_2$ in precisely one point, which must be red. Therefore there are at least $3q - |\mathcal{B}| + 1 > 0$ red points in $\mathcal{B}_2$. Conversely, starting from a red point in $\mathcal{B}_2$, we see that there are at least $3q - |\mathcal{B}| + 1$ red points in $\mathcal{B}_1$. Hence the number of red points is at least $2(3q - |\mathcal{B}| + 1)$. As this argument is valid for the number of green points as well, $|\mathcal{B}| \ge 4(3q - |\mathcal{B}| + 1)$ holds, thus $|\mathcal{B}| > \frac{12}{5}q$. □

This is enough to prove Theorem 5.1.8 if q is a square.

THEOREM 5.1.8 (first case, [B]). *Let $q > 256$ be a square prime power. Then* $\mathrm{UCN}(\mathrm{PG}(2, q)) = v - \tau_2 + 1 = q^2 - q - 2\sqrt{q}$. *Equality can be reached only by a trivial coloring.*

Proof. Result 1.5.7 yields $\tau_2 = 2q + 2\sqrt{q} + 2$. Let $\mathcal{C}$ be a nontrivial proper coloring of $v - \tau_2 + 1 + e$ colors. Suppose to the contrary that $e \ge 0$. By Lemma 5.2.3, we may assume that there is at most one 2-class in $\mathcal{C}$, and the nontriviality of the coloring is also preserved as $\tau_2 = 2q + 2\sqrt{q} + 2 < 3q$.

Suppose that $|\mathcal{B}| \geq 3q - 3$. Then $\alpha = 3$ and $c_0 = 2.5$ are convenient for Proposition 5.2.5: $\tau_2 = 2q + 2\sqrt{q} + 2 \leq 2.5q - 10/3$ for $q \geq 36$, and $q(2.5) = 8$. Thus $e < 0$, a contradiction.

Now suppose $\tau_2 + 6 \leq |\mathcal{B}| \leq 3q - 4$. Then by Remark 5.2.7, we may use Proposition 5.2.8 to obtain

$$\frac{2}{3}(|\mathcal{B}| - \tau_2)(3q - |\mathcal{B}| + 2) \leq \tau_2.$$

As the left-hand side is concave in $|\mathcal{B}|$, it is enough to obtain a contradiction for the values $|\mathcal{B}| = \tau_2 + 6$ and $|\mathcal{B}| = 3q - 4$. Substituting either values of $|\mathcal{B}|$ we get $4(3q - \tau_2 - 4) \leq \tau_2$, thus $12q/5 - 5 < \tau_2 = 2q + 2\sqrt{q} + 2$, a contradiction even for $q \geq 49$.

Finally, suppose $|\mathcal{B}| \leq \tau_2 + 5$. By Remark 1.5.9, $\mathcal{B}$ contains the union of two disjoint Baer subplanes, which is a minimal double blocking set. Thus Proposition 5.2.9 yields $\tau_2 + 5 \geq |\mathcal{B}| > 12q/5$, a contradiction. □

In Proposition 5.2.9 we relied on the assumption that a small double blocking set contains two disjoint blocking sets, and this could be used to find large color classes. If q is not a square, we do not know whether small double blocking sets have this property. Thus we need further investigations and the $t \pmod p$ result on small t-fold blocking sets (Result 1.5.10) to find at least one large color class, and to obtain a result similar to Proposition 5.2.9.

PROPOSITION 5.2.10 ([B]). *Let $\mathcal{C}$ be a nontrivial proper coloring. Let $\xi \in \mathbb{N}$. Suppose that $|\mathcal{B}| \leq \tau_2 + \xi < 2q + (q+3)/2$ and $\xi \leq (\tau_2 - 2q)/24$. Then $\tau_2 > 3q/2 + pq/50 - \xi + 1$, where p is the characteristic of the field.*

Proof. As $|\mathcal{B}| < 3q$, the set $\mathcal{B}'$ of essential points of $\mathcal{B}$ is a double blocking set (Corollary 2.1.3). As $\mathcal{C}$ is nontrivial, $\mathcal{B}'$ cannot be monochromatic (Proposition 5.2.2). By merging color classes while preserving this property, we may assume that there are only two color classes inside $\mathcal{B}$, say, red and green, each containing at least one essential point of $\mathcal{B}$. (We do not want to preserve the number of colors this time.) By Result 1.5.10, if a line ℓ intersects $\mathcal{B}'$ in more than two points, then $|\ell \cap \mathcal{B}'| \geq p + 2$. We refer to such lines as long secants. We are about to find a red point on which there are many long secant lines that have at least as many red points as green.

Let $|\mathcal{B}'| = b \geq \tau_2 \geq 2(q+1)$. Denote the set of red and green essential points by $\mathcal{B}_r$ and $\mathcal{B}_g$, respectively, and for any line $\ell \in \mathcal{L}$, let $n_\ell = |\ell \cap \mathcal{B}'|$, $n_\ell^r = |\ell \cap \mathcal{B}_r|$ and $n_\ell^g = |\ell \cap \mathcal{B}_g|$. Clearly $n_\ell = n_\ell^r + n_\ell^g$ for all line ℓ. Using double counting we get $\sum_{\ell \in \mathcal{L}} n_\ell = |\mathcal{B}'|(q+1)$, hence

$$\sum_{\ell \in \mathcal{L}\colon n_\ell > 2} n_\ell \geq \sum_{\ell \in \mathcal{L}} (n_\ell - 2) = b(q+1) - 2v = bq + 2(q+1) - 2(q^2+q+1) \geq (b-2q)q.$$

Let $\mathcal{L}^r = \{\ell \in \mathcal{L}\colon |\ell \cap \mathcal{B}'| > 2, n_\ell^r > n_\ell^g\}$, $\mathcal{L}^g = \{\ell \in \mathcal{L}\colon |\ell \cap \mathcal{B}'| > 2, n_\ell^r < n_\ell^g\}$, and $\mathcal{L}^= = \{\ell \in \mathcal{L}\colon, n_\ell^r = n_\ell^g\}$. Then

$$(b-2q)q \leq \sum_{\ell \in \mathcal{L}\colon n_\ell > 2} n_\ell = \sum_{\ell \in \mathcal{L}^r} (n_\ell^r + n_\ell^g) + \sum_{\ell \in \mathcal{L}^g} (n_\ell^r + n_\ell^g) + \sum_{\ell \in \mathcal{L}^=} (n_\ell^r + n_\ell^g) \leq$$

$$\sum_{\ell \in \mathcal{L}^r} 2n_\ell^r + \sum_{\ell \in \mathcal{L}^g} 2n_\ell^g + \sum_{\ell \in \mathcal{L}^=} 2n_\ell^r \leq 4 \cdot \sum_{\ell \in \mathcal{L}^r \cup \mathcal{L}^=} n_\ell^r,$$

where we assumed in the last step that the first sum was at least as large as the second (we may interchange the colors without the loss of generality). We say that a line ℓ is red if $n_\ell^r \geq n_\ell^g$. Hence, by the above inequality, there exists a point $P \in \mathcal{B}_r$ such that the number of long secant red lines passing through P is at least $(b-2q)q/4|\mathcal{B}_r| \geq (\tau_2 - 2q)q/4|\mathcal{B}_r|$. On these lines there are at least $p/2$ red points besides P. Moreover, on the two-secants to $\mathcal{B}$ through P, there are at least $3q - |\mathcal{B}| + 1$ red points besides P (see Proposition 5.2.6). Thus we have $|\mathcal{B}_r| \geq (\tau_2 - 2q)pq/8|\mathcal{B}_r| + 3q - |\mathcal{B}| + 2$. As there exists a green essential point, Proposition 5.2.6 yields that the total number γ of green points in $\mathcal{B}$ is at least $3q - |\mathcal{B}| + 2$. Therefore, $|\mathcal{B}_r| \leq |\mathcal{B}| - \gamma \leq 2|\mathcal{B}| - 3q - 2$. Thus altogether we have $(\tau_2 - 2q)pq/8|\mathcal{B}_r| + 3q - |\mathcal{B}| + 2 \leq 2|\mathcal{B}| - 3q - 2$, hence $(\tau_2 - 2q)pq/8|\mathcal{B}_r| \leq 3|\mathcal{B}| - 6q - 4 < 3(\tau_2 - 2q + \xi)$. Therefore

$$\frac{(\tau_2 - 2q)pq}{24(\tau_2 - 2q + \xi)} < |\mathcal{B}_r| \leq 2|\mathcal{B}| - 3q - 2 = 2\tau_2 - 3q + 2\xi - 2.$$

Since $\xi \leq (\tau_2 - 2q)/24$, we have $24(\tau_2 - 2q + \xi) \leq 25(\tau_2 - 2q)$, hence the assertion $pq/50 + 3q/2 - \xi + 1 < \tau_2$ follows. □

Now we are ready to prove the second (and last) part of Theorem 5.1.8.

Theorem 5.1.8 (second case, [B]). *Suppose that $q = p^h$, $p \geq 29$ prime, $h \geq 3$ odd. Then* $\mathrm{UCN}(\mathrm{PG}(2,q)) = v - \tau_2 + 1$, *and equality can be reached only by a trivial coloring.*

Proof. Corollary 2.2.2 yields $\tau_2 \leq 2q+2(q-1)/(p-1)$. As $p \geq 29$, $\tau_2 < 2q+q/14$. Note that $q \geq p^3 > 20000$ is fairly large. Suppose to the contrary that $\mathcal{C}$ is a nontrivial proper coloring with $e = e(\mathcal{C}) \geq 0$. By Lemma 5.2.3, we may assume that there is at most one 2-class in $\mathcal{C}$, and the nontriviality of the coloring is also preserved as $\tau_2 < 3q$.

First suppose that $|\mathcal{B}| \geq 3q - 11$. Then $\alpha = 11$ and $c_0 = 2.5$ are convenient for Proposition 5.2.5: $\tau_2 < 2q + q/14 \leq 2.5q - 26/3$, and $q(2.5) = 8$. Thus $e < 0$, a contradiction.

Now suppose $\tau_2 + 12 \leq |\mathcal{B}| \leq 3q - 12$. Then by Remark 5.2.7, we may use Proposition 5.2.8 to obtain

$$\frac{2}{3}(|\mathcal{B}| - \tau_2)(3q - |\mathcal{B}|) < \tau_2.$$

As the left-hand side is concave in $|\mathcal{B}|$, it is enough to obtain a contradiction for the values $|\mathcal{B}| = \tau_2 + 12$ and $|\mathcal{B}| = 3q - 12$. Substituting either values of $|\mathcal{B}|$, we get $8(3q - \tau_2 - 12) \leq \tau_2$, thus $24q/9 - 11 < \tau_2 < 2q + q/14$, a contradiction.

Thus $|\mathcal{B}| \leq \tau_2 + 11 < 2q + (q+3)/2$. By Result 1.5.8, we have $(\tau_2 - 2q)/24 > q^{2/3}/24 \geq 29^2/24 > 29$, thus we may apply Proposition 5.2.10 with $\xi = 11$ to obtain $\tau_2 > 3q/2 + pq/50 - 10 \geq 2q + 2q/25 - 10$. Compared to $\tau_2 < 2q + q/14$, q is large enough to get a contradiction. $\square$

5.3 Remarks

Again, if we knew that the double blocking sets of size $\tau_2(\mathrm{PG}(2,q))$ in PG$(2,q)$ are the union of two disjoint blocking sets, then we could use Proposition 5.2.9 instead of Proposition 5.2.10 to obtain the result of Theorem 5.1.8 under less restrictive assumptions. The conditions of Theorem 5.1.8 on q and p are rather technical, and it is very likely that they are not sharp, yet some restrictions are necessary. Let P_1, P_2, P_3 be three non-collinear points, and let $\ell_1 = P_2P_3$, $\ell_2 = P_1P_3$, $\ell_3 = P_1P_2$. Then the triangle $\ell_1 \cup \ell_2 \cup \ell_3$ is a minimal double blocking set of size $3q$. It is easy to see that the coloring in which the color classes of size at least two are $\ell_2 \cup \ell_3 \setminus \{P_1\}$ and $\{P_1\} \cup \ell_1 \setminus \{P_2, P_3\}$ is proper, and it uses $v - 3q + 2$ colors. However, $\tau_2(\mathrm{PG}(2,q)) = 3q$ for $2 \leq q \leq 8$ (cf. [13]), thus in these cases the conclusion of Theroem 5.1.8 fails. For arbitrary finite projective planes, the results of Theorems 5.1.7 and 5.1.8 may be false or hopeless to prove.

Chapter 6

The Zarankiewicz problem

6.1 Introduction

This chapter is based on [C]. $K_{n,m}$ denotes the complete bipartite graph in which the vertex classes have n and m elements, respectively. C_n denotes the cycle of length n. Note that $K_{2,2}$ is isomorphic to C_4. The number of edges of a graph G will be denoted by $e(G)$.

DEFINITION 6.1.1. *A bipartite graph $G = (A, B; E)$ is $K_{\alpha,\beta}$*-free *if it does not contain α nodes in A and β nodes in B that span a subgraph isomorphic to $K_{\alpha,\beta}$. We call $(|A|, |B|)$ the* size *of G. The maximum number of edges a $K_{\alpha,\beta}$-free bipartite graph of size (m, n) may have is denoted by $Z_{\alpha,\beta}(m, n)$, and is called a* Zarankiewicz number*. Graphs attaining equality are called* extremal.

Note that a $K_{s,t}$-free bipartite graph is not necessarily $K_{t,s}$-free if $s \neq t$. The problem of determining $Z_{\alpha,\beta}(m, n)$ is known as Zarankiewicz's problem [77], though originally it was formulated via matrices in the following way: what is the minimum number of 1's in a 0-1 matrix of dimension $m \times n$ that ensures the existence of an $\alpha \times \beta$ submatrix containing only 1s? This quantity is denoted by $K(m, n, \alpha, \beta)$, and it clearly equals $Z_{\alpha,\beta}(m, n) + 1$. The history of the problem and early results are collected in Guy [43] (1969). We do not know of a more recent survey in the topic, so we refer the interested reader to the works of Irving [50], Füredi [39, 40], Alon–Rónyai–Szabó [3], Nikiforov [59], Griggs–Ho [42], Balbuena–García-Vázquez–Marcote–Valenzuela [11], and the references therein. Determining the exact value of $Z_{\alpha,\beta}(m, n)$ is extremely hard in general. However, if one of the vertex classes is much bigger than the other one, or the parameters fit those of a block design, exact results are known.

RESULT 6.1.2 (Čulík [30]). *If* $1 \le s \le m$ *and* $n \ge (t-1)\binom{m}{s}$, *then*

$$Z_{s,t}(m,n) = (s-1)n + (t-1)\binom{m}{s}.$$

RESULT 6.1.3 (Guy [43]). *If* $\ell(n,s,t) \le n \le (t-1)\binom{m}{s} + 1$, *then*

$$Z_{s,t}(m,n) = \left\lfloor \frac{(s^2-1)n + (t-1)\binom{m}{s}}{s} \right\rfloor,$$

where $\ell(n,s,t)$ *is approximately* $(t-1)\binom{m}{s}/(s+1)$.

DEFINITION 6.1.4. *Let* $\emptyset \ne K \subset \mathbb{Z}^+$. *An incidence structure* $(\mathcal{P},\mathcal{B})$ *is called a* t-(v,K,λ) design, *if* $|\mathcal{P}| = v$, $\forall B \in \mathcal{B}$: $|B| \in K$, *and every* t *distinct points are contained in precisely* λ *distinct blocks. If* $K = \{k\}$, *we write simply* t-(v,k,λ).

In a t-(v,k,λ) design, the total number $|\mathcal{B}| = b$ of blocks is $b = \lambda\binom{v}{t}/\binom{k}{t}$, and the number r of blocks incident with an arbitrary fixed point is $r = bk/v = \lambda\binom{v-1}{t-1}/\binom{k-1}{t-1}$. We always assume that $k < v$. The incidence graph of a t-(v,k,λ) design is $K_{t,\lambda+1}$-free of size (v,b) by definition, and they turn out to have the most possible number of edges among such graphs. Special cases of the next result were also established earlier by Reiman [63, 64], Kárteszi [52, 53] and Hyltén-Cavallius [48].

RESULT 6.1.5 (Roman's bound [65]). *Let* $G = (A,B;E)$ *be a* $K_{s,t}$*-free bipartite graph of size* (m,n), *and let* $p \ge s-1$, $p \in \mathbb{N}$. *Then the number of edges in* G *satisfy*

$$e(G) \le R(s,t,m,n,p) := \frac{(t-1)}{\binom{p}{s-1}}\binom{m}{s} + n \cdot \frac{(p+1)(s-1)}{s}.$$

Equality holds if and only if every vertex in B *has degree* p *or* $p+1$ *and every* s*-tuple in* A *has exactly* $t-1$ *common neighbors in* B.

The proof of the above result is based on the following estimation (cf. [55]): the number of $K_{1,s}$s in G is exactly $\sum_{v\in B}\binom{d(v)}{s}$; on the other hand, it is at most $(t-1)\binom{m}{s}$ (as no s-tuple in A may have t common neighbors). Thus we are to estimate $\sum_{v\in B} d(v)$ subject to $\sum_{v\in B}\binom{d(v)}{s} \le (t-1)\binom{m}{s}$. This can be done, e.g., by applying Jensen's inequality to the convex extension of $\binom{x}{s}$, but it is somewhat uncomfortable. The ready-to-use formulation above, in fact, can be derived from Jensen's inequality for integers, though Roman used other ideas to prove it.

The existence of designs with given parameters is also a very hard question in general. We will use only a trivial necessary condition.

DEFINITION 6.1.6. *We call the parameters* (t, v, k, λ) admissible*, if they are positive integers satisfying* $2 \le t$*,* $t \le k < v$*, furthermore,* $b := \lambda\binom{v}{t}/\binom{k}{t}$ *and* $r := bk/v = \lambda\binom{v-1}{t-1}/\binom{k-1}{t-1}$ *are also integers.*

REMARK 6.1.7. *If* (t, v, k, λ) *are admissible parameters in the sense of Definition 6.1.6, then* $R(t, \lambda + 1, v, b, k) = bk = rv$ *is integer.*

A projective plane of order q can be considered as a 2-$(q^2 + q + 1, q + 1, 1)$ design. The main concept of this chapter is to look for C_4-free graphs with many edges as subgraphs of the incidence graph of a projective plane.

6.2 Constructions and bounds

The incidence graphs of t-$(v, \{k, k + 1\}, \lambda)$ designs are $K_{t,\lambda+1}$-free, and these are precisely the graphs that satisfy the conditions of equality in Roman's bound, thus they are extremal. Next we give some examples of such structures.

EXAMPLE 6.2.1. *a) If we delete one point arbitrarily from a* t-(v, k, λ) *design, we obtain a* t-$(v - 1, \{k - 1, k\}, \lambda)$ *design.*

b) Take a 2-$(v, k, 1)$ *design* $\mathcal{D}$ *and delete a block from it with all, or all but one of its points. We obtain a* 2-$(v - k + c, \{k - 1, k\}, 1)$ *design,* $c \in \{0, 1\}$*.*

c) Delete two intersecting lines ℓ_1*,* ℓ_2 *with all their points except possibly one point* $P \neq \ell_1 \cap \ell_2$ *from an affine plane of order* n *(that is, a* 2-$(n^2, n, 1)$ *design, where* $r = n + 1$*). In this way we get a* 2-$(n^2 - 2n + 1 + c, \{n - 2, n - 1\}, 1)$ *design* $\mathcal{D}'$*,* $c \in \{0, 1\}$*. Note that if* $c = 0$*, then every point of* $\mathcal{D}'$ *has degree* r*, while for* $c = 1$*, one point has degree* $r - 1$ *(this holds in Example b) as well).*

d) Let $\mathcal{O}$ *be an oval in a projective plane* Π_q *of order* q*,* q *odd, and let* $\mathcal{S} \subset \mathcal{O}$ *be any point-set. Let* $\mathcal{P}_0 = \mathrm{Inn}(\mathcal{O}) \cup \mathcal{S}$*,* $\mathcal{L}_0 = \mathrm{Skw}(\mathcal{O}) \cup \mathrm{Sec}(\mathcal{O})$*, and consider the subgraph of* Π_q *induced by* $\mathcal{P}_0 \cup \mathcal{L}_0$ *(that is, we delete the tangents of* $\mathcal{O}$*, the outer points of* $\mathcal{O}$*, and some points of* $\mathcal{O}$*). As no point of* $\mathrm{Inn}(\mathcal{O})$ *is incident with a tangent of* $\mathcal{O}$*, any two points of* $\mathcal{P}_0$ *are connected by a line of* $\mathcal{L}_0$*. Note that the points of* $\mathrm{Inn}(\mathcal{O})$ *have degree* $q + 1$*, while the points of* $\mathcal{S}$ *have degree* q*. A skew line has precisely* $(q + 1)/2$ *points in* $\mathcal{P}_0$*, while a line* $\ell \in \mathrm{Sec}(\mathcal{O})$ *has* $(q - 1)/2 + |\ell \cap \mathcal{S}|$ *points in* $\mathcal{P}_0$*, which is zero or one if* $|\mathcal{S}| \in \{0, 1\}$*, and one or two if* $|\mathcal{S}| \in \{q, q + 1\}$*; thus for* $|\mathcal{S}| \le 1$ *and* $|\mathcal{S}| \ge q$ *we obtain a* 2-$(|\mathcal{S}| + q(q - 1)/2, \{(q - 1)/2, (q + 1)/2\}, 1)$ *and a* 2-$(|\mathcal{S}| + q(q - 1)/2, \{(q + 1)/2, (q + 3)/2\}, 1)$ *design, respectively.*

As seen in Example a), Roman's bound yields that if we remove one point from a design, the resulting graph is also extremal. The next result, which is also a direct consequence of Roman's bound, shows that we may go further.

PROPOSITION 6.2.2 ([C]). *Assume that the parameters* (t,v,k,λ) *are admissible, and let* c_0 *be the largest integer such that* $\lambda\left(\binom{v-c_0}{t}+c_0\binom{v-1}{t-1}-\binom{v}{t}\right)<\binom{k-1}{t-1}$. *Then for every integer* $0\le c\le c_0$,

$$Z_{t,\lambda+1}(v-c,b)\le r(v-c).$$

Equality can be reached if a t-(v,k,λ)*-design exists. Moreover, if* $c<c_0$*, then in the graphs obtaining equality, the vertices in the class of size* $v-c$ *have degree* r*. In particular, the condition for* $t=2$ *is* $c_0(c_0-1)<2(k-1)/\lambda$.

Proof. Removing c points from the incidence graph of a t-(v,k,λ) design we obtain a $K_{t,\lambda+1}$-free graph on $(v-c,b)$ nodes and $r(v-c)$ edges.

On the other hand, using $rv=bk$ and $bk/t=\lambda\binom{v}{t}/\binom{k-1}{t-1}$, Roman's bound with $p=k-1$ yields $Z_{t,\lambda+1}(v-c,b)\le$

$$\left\lfloor\frac{\lambda}{\binom{k-1}{t-1}}\binom{v-c}{t}+b\cdot\frac{k(t-1)}{t}\right\rfloor=r(v-c)+\left\lfloor\frac{\lambda\left(\binom{v-c}{t}+c\binom{v-1}{t-1}-\binom{v}{t}\right)}{\binom{k-1}{t-1}}\right\rfloor.$$

Suppose that $G=(A,B)$ is $K_{t,\lambda+1}$-free on $(v-c,b)$ vertices and $(v-c)r$ edges, $c<c_0$. Assume that there is a vertex $u\in A$ with degree smaller than r. Removing u from A, we obtain a graph on $(v-c-1,b)$ vertices and more than $(v-c-1)r$ edges, which contradicts our upper bound. $\square$

For a projective plane of order n, the bound on c in the above proposition is roughly $\sqrt{2n}$. To prove a stronger result, we need a theorem of Metsch and a slight relaxation of it.

RESULT 6.2.3 (Metsch [58]). *Let* $n\ge 15$, $(\mathcal{P},\mathcal{L},\mathcal{I})$ *be an incidence structure with* $|\mathcal{P}|=n^2+n+1$, $|\mathcal{L}|\ge n^2+2$ *such that every line in* $\mathcal{L}$ *is incident with* $n+1$ *points of* $\mathcal{P}$ *and every two lines have at most one point in common. Then a projective plane* Π *of order* n *exists and* $(\mathcal{P},\mathcal{L},\mathcal{I})$ *can be embedded into* Π.

LEMMA 6.2.4 ([C]). *Let* $n\ge 15$, $G=(\mathcal{P},\mathcal{L};\mathcal{I})$ *be an incidence graph with* $|\mathcal{P}|=n^2+n+1$, $|\mathcal{L}|\ge n^2+2$ *such that every line in* $\mathcal{L}$ *is incident with* at least $n+1$ *points of* $\mathcal{P}$*, and every two lines have at most one point in common. Then a projective plane* Π *of order* n *exists, and* $(\mathcal{P},\mathcal{L},\mathcal{I})$ *can be embedded into* Π*; in particular, every line in* $\mathcal{L}$ *is incident with exactly* $n+1$ *points of* $\mathcal{P}$.

Proof. By deleting edges from G, we can obtain a graph $G' = (\mathcal{P}, \mathcal{L}, \mathcal{I}')$ in which the vertices of $\mathcal{L}$ have degree exactly $n+1$. Then, by Theorem 6.2.3, G' is a subgraph of a projective plane Π of order n. Now suppose that there is a line ℓ in $\mathcal{L}$ that has degree at least $n+2$ in G. This means that there exists a point P such that ℓ is incident with P in G, but not in Π. Then each of the $n+1$ lines passing through P in Π intersects ℓ in a point different from P. As $|\mathcal{L}| \geq n^2+1$, at least one of these lines is a line of G as well, but it intersects ℓ in at least two points in G, a contradiction. Hence every line has $n+1$ points in G. $\square$

THEOREM 6.2.5 ([C]). *Let $n \geq 15$, and $c \leq n/2$, $0 \leq c \in \mathbb{Z}$. Then*

$$Z_{2,2}(n^2+n+1-c, n^2+n+1) \leq (n^2+n+1-c)(n+1).$$

Equality holds if and only if a projective plane of order n exists. Moreover, graphs giving equality are subgraphs of a projective plane of order n.

Proof. If a projective plane of order n exists, deleting c of its lines yields a graph on $(n^2+n+1-c, n^2+n+1)$ vertices and $(n^2+n+1-c)(n+1)$ edges.

Suppose that $G = (A, B; E)$ is a $K_{2,2}$-free graph on $(n^2+n+1-c, n^2+n+1)$ vertices and $e(G) \geq |A|(n+1)$ edges. Let m be the number of vertices in A of degree at most n (low-degree vertices). Assume that $m \geq n-c$. Delete $(n-c)$ low-degree vertices to obtain a graph G' on (n^2+1, n^2+n+1) vertices with at least $(n^2+1)(n+1)+(n-c)$ edges. By Roman's bound with $p = n$, $Z_{2,2}(n^2+1, n^2+n+1) \leq (n^2+1)(n+1)+(n-1)/2$, hence $n-c \leq (n-1)/2$. This contradicts $c \leq n/2$, thus $m < n-c$ must hold.

Now delete all the low-degree vertices from A to obtain a graph G' on the vertex sets (A', B) with $|A'| \geq n^2+2$, $|B| = n^2+n+1$. Then every vertex in A' has degree at least $n+1$, hence we can apply Lemma 6.2.4 to derive that G' can be embedded into a projective plane Π of order n, therefore every vertex in A' has degree $n+1$, which combined with $e(G) \geq |A|(n+1)$ yields that every vertex in A has degree $n+1$ (in G), thus G itself can be embedded into Π. $\square$

REMARK 6.2.6. *If we knew $Z_{2,2}(n^2+1, n^2+n+1) \leq (n^2+1)(n+1)+\delta$, then the above argument would hold for $c < n-\delta$. Removing n points (or lines) from a projective plane of order n we get $Z_{2,2}(n^2+1, n^2+n+1) \geq (n^2+1)(n+1)$. Note that an affine plane plus an extra line containing a single point shows $Z_{2,2}(n^2, n^2+n+1) \geq n^2(n+1)+1$, thus Theorem 6.2.5 cannot be extended to $c = n+1$.*

QUESTION 6.2.7. *Is it true that $Z_{2,2}(n^2+1, n^2+n+1) \leq (n^2+1)(n+1)$ (if n is large enough)?*

If an extremal graph is embedded into another one, it is easier to figure out how could we extend it to a larger one with many edges. Classical unitals show such an example.

THEOREM 6.2.8. *Let q be a square prime power, and let $c(c-1) < 2(\sqrt{q}+1)$, $0 \leq c \in \mathbb{Z}$. Then*

$$Z_{2,2}(q\sqrt{q}+1+c, q(q-\sqrt{q}+1)) = q(q\sqrt{q}+1) + c(q-\sqrt{q}+1).$$

Proof. Let $\mathcal{U}$ be a classical unital in $\mathrm{PG}(2,q)$ (that is, the set of the $\mathrm{GF}(q)$-rational points of an Hermitian curve). Recall that every line intersects $\mathcal{U}$ in either one or $\sqrt{q}+1$ points; the number of tangents to $\mathcal{U}$ through a point P is one or $\sqrt{q}+1$ depending on whether $P \in \mathcal{U}$ or $P \notin \mathcal{U}$; and the points of $\mathcal{U}$ together with the $q(q-\sqrt{q}+1)$ long secants to $\mathcal{U}$ form a 2-$(q\sqrt{q}+1, \sqrt{q}+1, 1)$ design. Let $G = (\mathcal{U}, \mathcal{L})$ be the incidence graph of this design. Another well-known property of $\mathcal{U}$ is that if we take any point P not belonging to $\mathcal{U}$, then the $\sqrt{q}+1$ points of $\mathcal{U}$ that are on the tangents to $\mathcal{U}$ through P, called the feet of P, are collinear [46]. Now take a tangent line $\ell = \{P_0, P_1, \ldots, P_q\}$ to $\mathcal{U}$ and suppose that $\ell \cap \mathcal{U} = P_0$. Let e_i be the unique long secant to $\mathcal{U}$ such that $e_i \cap \mathcal{U}$ are the feet of P_i. It is clear that $P_i \notin e_j$ for all $1 \leq i, j \leq q$, otherwise we would have $\{P_0, P_i\} \subset \ell \cap e_j$. Consider the subgraph of $\mathrm{PG}(2,q)$ induced by $\mathcal{U} \cup \{P_1, \ldots, P_q\} \cup \mathcal{L}$, and add an edge between P_i and e_i for all $1 \leq i \leq q$ (that is, we add a matching of size q). Let this new graph be G^*. Then in G^*, the points of $\mathcal{U}$ have degree q, while the P_is have degree $q-\sqrt{q}+1$. Now suppose that we have a C_4 in G^* induced by P, Q, e, and f. As a new edge must be involved in the C_4, but no more than one can be involved, we may assume that $P = P_i$ and $e = e_i$. Then $Q \in e_i$ is a point of $\mathcal{U}$, and f must be the original long secant connecting P_i and Q. This is a contradiction as P_iQ is a tangent to $\mathcal{U}$. Thus $Z_{2,2}(q\sqrt{q}+1+c, q(q-\sqrt{q}+1)) \geq q(q\sqrt{q}+1)+c(q-\sqrt{q}+1)$ for all $0 \leq c \leq q$. On the other hand, by Roman's bound we have

$$Z_{2,2}(q\sqrt{q}+1+c, q(q-\sqrt{q}+1)) \leq R(2,2,q\sqrt{q}+1+c, q(q-\sqrt{q}+1), \sqrt{q}+1) =$$

$$q(q\sqrt{q}+1) + c(q-\sqrt{q}+1) + \frac{c(c-1)}{2(\sqrt{q}+1)}.$$

□

We have seen that if we delete the lowest degree vertex from an extremal $K_{s,t}$-free graph, the resulting graph is also $K_{s,t}$-free and it has considerably many edges (sometimes also extremal). This was also pointed out by Guy [43, p138, point C]. Despite its triviality, this idea turns out surprisingly useful. From now on, $\mathcal{F}$ denotes a subgraph-closed family of bipartite graphs; that is, if $G \in \mathcal{F}$ and H is a subgraph of G, then $H \in \mathcal{F}$. For example, $K_{s,t}$-free graphs clearly form a subgraph-closed family. Let $\mathcal{F}(m,n) = \{(A,B;E) \in \mathcal{F} \colon |A| = m, |B| = n\}$, $\mathrm{ex}_{\mathcal{F}}(m,n) = \max\{e(G) \colon G \in \mathcal{F}(m,n)\}$, and let $\mathrm{Ex}_{\mathcal{F}}(m,n) = \{G \in \mathcal{F}(m,n) \colon e(G) = \mathrm{ex}_{\mathcal{F}}(m,n)\}$. Graphs of $\mathrm{Ex}_{\mathcal{F}}(m,n)$ are called extremal.

THEOREM 6.2.9 ([C]). *Let $\mathcal{F}$ be a subgraph-closed family of bipartite graphs. Suppose that $\mathrm{ex}_{\mathcal{F}}(m,n) \le e$, and let $0 \le c \in \mathbb{Z}$. Then*

(1) $\mathrm{ex}_{\mathcal{F}}(m+c,n) \le e + c\lfloor e/m \rfloor$*;*

(2) $\mathrm{ex}_{\mathcal{F}}(m,n+c) \le e + c\lfloor e/n \rfloor$*.*

Moreover, if equality holds in, say, (1) for some $c \ge 1$, then equality holds for all $c' \in \mathbb{Z}$, $0 \le c' < c$ as well, and any graph $G \in \mathrm{Ex}_{\mathcal{F}}(m+c,n)$ induces a subgraph that is in $\mathrm{Ex}_{\mathcal{F}}(m+c-1,n)$.

Proof. It is enough to prove (1) as (2) is completely analogous. We prove the assertion by induction on c. The statement is trivial if $c = 0$. Let $d = \lfloor e/m \rfloor$. Suppose $\mathrm{ex}_{\mathcal{F}}(m+c,n) \ge e + cd$, and let $G = (A,B;E) \in \mathrm{Ex}_{\mathcal{F}}(m+c,n)$. There is no vertex of degree strictly smaller than d in A, otherwise removing such a vertex we would obtain a graph in $\mathcal{F}(m+c-1,n)$ with more than $e+(c-1)d$ edges, which is not possible by the inductive hypothesis. Consider an arbitrary subgraph of G on (m,n) vertices. By the definition of d, we find a vertex in A of degree d. Removing this vertex, we obtain a graph G' of $\mathcal{F}(m+c-1,n)$ with at least, hence (by the inductive hypothesis) exactly $e+(c-1)d$ edges. Thus $\mathrm{ex}_{\mathcal{F}}(m+c-1,n) = e+(c-1)d = e(G')$, and $\mathrm{ex}_{\mathcal{F}}(m+c,n) = e(G) = e+cd$. □

Sometimes it is more comfortable to use the following form of Theorem 6.2.9.

REMARK 6.2.10. *Let $0 \le c, d \in \mathbb{Z}$. Suppose that $\mathrm{ex}_{\mathcal{F}}(m,n) \le md$ and $\mathrm{ex}_{\mathcal{F}}(m+1,n) < (m+1)d$. Then $\mathrm{ex}_{\mathcal{F}}(m+c,n) \le md + c(d-1)$. In case of equality the same holds as in Theorem 6.2.9.*

Proof. The conditions imply that we may use Theorem 6.2.9 starting from either $\mathrm{ex}_{\mathcal{F}}(m,n)$ or $\mathrm{ex}_{\mathcal{F}}(m+1,n)$. □

By the above remark, Theorem 6.2.9 is especially useful if we have an extremal graph from a family $\mathcal{F}$ such that one of its vertex classes is regular of some degree d, we can extend that class by adding further vertices of degree $d-1$ (while still remaining in $\mathcal{F}$), and the first extension is also extremal.

COROLLARY 6.2.11 ([C]). *(1) Let* (t, v, k, λ) *be admissible parameters (with* $b = \lambda\binom{v}{t}/\binom{k}{t}$, $r = \lambda\binom{v-1}{t-1}/\binom{k-1}{t-1}$*), and let* $0 \le c \in \mathbb{Z}$. *Then*

$$Z_{t,\lambda+1}(v + c, b) \le rv + c(r - 1). \tag{6.1}$$

(2) Let $(2, v, k, 1)$ *be admissible parameters. Then*

$$Z_{2,2}(v - k + c, b - 1) \le (v - k)r + c(r - 1). \tag{6.2}$$

Moreover, if a 2-$(v, k, 1)$ *design exists, then equality holds in* (6.2) *for all* $0 \le c \le k$.

Proof. (1) Roman's bound yields $rv = R(t, \lambda + 1, v, b, k) = \lambda\binom{v}{t}/\binom{k}{t-1} + b(k + 1)(t - 1)/t$, furthermore

$$Z_{2,\lambda+1}(v+1, b) \le R(t, \lambda+1, v+1, b, k) = \lambda\frac{\binom{v+1}{t}}{\binom{k}{t-1}} + \frac{b(k + 1)(t - 1)}{t} = rv + \lambda\frac{\binom{v}{t-1}}{\binom{k}{t-1}}.$$

It is easy to see that $r > \lambda\binom{v}{t-1}/\binom{k}{t-1}$, so Remark 6.2.10 applies.
(2) Example 6.2.1 **b)** shows $Z_{2,2}(v - k, b - 1) \le e := R(2, 2, v - k, b - 1, k - 1) = (v - k)r$ and $Z_{2,2}(v - k + 1, b - 1) \le e + (r - 1)$, thus Remark 6.2.10 applies. If a 2-$(v, k, 1)$ design exists, we may remove one of its blocks and all but c points of that block to obtain a graph with equality. □

COROLLARY 6.2.12. *Let* $0 \le c \in \mathbb{Z}$, q *odd. Then*

$$Z_{2,2}\left(\frac{q(q - 1)}{2} + c, q^2\right) \le \frac{(q^2 + 2c - 1)q}{2}.$$

Equality holds for $0 \le c \le q + 1$ *if there exists a projective plane of order* q *with an oval (e.g., if* q *is a prime power).*

Proof. Example 6.2.1 **d)** yields a construction attaining equality for all $0 \le c \le q + 1$. It also shows $R(2, 2, q(q - 1)/2 + c, q^2, (q - 1)/2) = (q + 1)q(q - 1)/2 + cq$ for $c = 0, 1$, hence Remark 6.2.10 proves the assertion for all $c \ge 0$. □

We remark that starting from PG(2, 5), Corollary 6.2.12 yields $Z_{2,2}(14, 25) = 80$. We easily find a line of degree two in the respective construction. Deleting this line, combined with Roman's bound, yields $Z_{2,2}(14, 24) = 78$. These Zarankiewicz numbers were reported inaccurately in [43].

In case of affine planes, we derive stronger results than Corollary 6.2.11. Recall that an affine plane of order n is always embeddable into a projective plane of order n. Totten [72] also has an embeddibility result on the complement of two lines in a projective plane (that is, we delete one line and all its points from an affine plane).

RESULT 6.2.13 (Totten [72]). *Let $\mathcal{S} = (\mathcal{P}, \mathcal{L})$ be a finite linear space (that is, an incidence structure where any two distinct points are contained in a unique line) with $|\mathcal{P}| = n^2 - n$, $|\mathcal{L}| = n^2 + n - 1$, $2 \leq n \neq 4$, and every point having degree $n + 1$. Then $\mathcal{S}$ can be embedded into a projective plane of order n.*

We slightly relax the conditions of this result (like we did with Metsch' one).

LEMMA 6.2.14 ([C]). *Let $\mathcal{S} = (\mathcal{P}, \mathcal{L})$ be a finite* partial *linear space (that is, an incidence structure where any two distinct points are contained in at most one line) with $|\mathcal{P}| = n^2 - n$, $|\mathcal{L}| = n^2 + n - 1$, $n > 4$, in which the number of flags is at least $(n^2 - n)(n + 1)$. Then $\mathcal{S}$ is a linear space, and it can be embedded into a projective plane of order n.*

Proof. As $R(2, 2, n^2 - n, n^2 + n - 1, n - 1) = (n^2 - n)(n + 1)$, each line in $\mathcal{L}$ has degree $n - 1$ or n, and any two distinct points must be contained in a unique line. The average degree of a point is $n + 1$. Now suppose that there is a point P of degree at least $n + 2$. Then the number of points on the lines incident with P is at least $1 + (n + 2)(n - 2) = n^2 - 3 > |\mathcal{P}| = n^2 - n$ (by $n > 4$). Hence every point has degree $n + 1$, so by Totten's Result 6.2.13, $\mathcal{S}$ is the complement of two lines in a projective plane of order n. $\square$

COROLLARY 6.2.15 ([C]). *Let $n \geq 2$ and $0 \leq c \in \mathbb{Z}$. Then*

$$Z_{2,2}(n^2 + c, n^2 + n) \leq n^2(n + 1) + cn, \tag{6.3}$$

$$Z_{2,2}(n^2 - n + c, n^2 + n - 1) \leq (n^2 - n)(n + 1) + cn, \tag{6.4}$$

$$Z_{2,2}(n^2 - 2n + 1 + c, n^2 + n - 2) \leq (n^2 - 2n + 1)(n + 1) + cn. \tag{6.5}$$

Equality can be reached in all three inequalities if a projective plane of order n exists and $c \leq n + 1$, $c \leq 2n$, or $c \leq 3(n - 1)$, respectively. Moreover, if $c \leq n + 1$, or $c \leq 2n$ and $n > 4$, then graphs reaching the bound in (6.3) *or* (6.4)*, respectively, can be embedded into a projective plane of order n.*

Proof. The parameters of an affine plane, $(2, n^2, n, 1)$ (with $b = n^2 + n$, $r = n + 1$) are admissible. Hence (6.3) and (6.4) follow from Corollary 6.2.11. To apply Theorem 6.2.9 in (6.5), it is enough to consider Example 6.2.1 c) and Remark 6.2.10.

By taking a projective plane of order n, and deleting one, two, or three of its lines and all but c of their points each of which is contained in only one of the deleted lines, we can reach equality in (6.3), (6.4), and (6.5), respectively, under the respective assumption on c.

In (6.3), Theorem 6.2.9 also provides an affine plane of order n as an induced subgraph in graphs obtaining equality. Now the c extra points of degree n must be incident with pairwise non-intersecting lines to avoid C_4's in the graph; that is, they can be considered as the common points of c distinct parallel classes. Adding the missing $n+1-c$ ideal points and the line at infinity, we obtain a projective plane of order n.

In (6.4), Theorem 6.2.9 provides us an extremal C_4-free subgraph $G=(A,B)$ on (n^2-n, n^2+n-1) vertices and $(n^2-n)(n+1)$ edges in graphs reaching equality. By Lemma 6.2.14, G can be embedded into a projective plane of order n. As before, it is easy to see that the embedding extends to the c extra points as well. $\square$

Next we prove a straightforward recursive inequality. For a bipartite graph $G=(A,B;E)$ and vertex-sets $X\subset A$ and $Y\subset B$, let $G[X,Y]$ denote the subgraph of G induced by $X\cup Y$.

PROPOSITION 6.2.16 ([C]). *Let $U_{s,t}(m,n,\alpha,\beta) = Z_{s-\alpha,t}(m-\alpha,\beta) + Z_{s,t}(m-\alpha, n-\beta) + (\alpha-1)n+\beta$. Then $Z_{s,t}(m,n)$ is at most*

$$\min_{\alpha}\max_{\beta}\min\{Z_{\alpha,\beta+1}(m,n),\, U_{s,t}(m,n,\alpha,\beta)\colon 1\le\alpha<s,\ t-1\le\beta\le n\}.$$

Proof. Let $G=(A,B;E)$ be a maximal $K_{s,t}$-free bipartite graph on $m+n$ vertices. Let $1\le\alpha<s$, and let β be the largest integer for which $K_{\alpha,\beta}$ is a subgraph of G (the ordering of the classes does matter). Then $|E|\le Z_{\alpha,\beta+1}(m,n)$ follows from G being $K_{\alpha,\beta+1}$-free. Now let $S\subset A$ and $T\subset B$ induce a $K_{\alpha,\beta}$, and let $U=A\setminus S$, $V=B\setminus T$. Then $G[U,T]$ must be $K_{s-\alpha,t}$-free; $G[U,V]$ is $K_{s,t}$-free; moreover, since no $K_{\alpha,\beta+1}$ can be found in G, every vertex in V may have at most $\alpha-1$ neighbors in S. Summing up the maximum number of edges in each part, we get $|E|\le\alpha\beta+Z_{s-\alpha,t}(m-\alpha,\beta)+Z_{s,t}(m-\alpha,n-\beta)+(\alpha-1)(n-\beta)=U_{s,t}(m,n,\alpha,\beta)$. As G is maximal, it must contain a $K_{\alpha,t-1}$ for all $\alpha<s$, hence we have $\beta\ge t-1$. $\square$

REMARK 6.2.17. *In particular, the case $\alpha=1$ of this inequality investigates the vertex with largest degree. $Z_{s,t}(m,0)$ is defined to be zero (which occurs above for*

$\beta = n$). Note that we may interchange the role of the classes, that is, write up the above inequality for $Z_{t,s}(n,m)$. We will call this the transpose *of Proposition 6.2.16.*

REMARK 6.2.18 ([C]). *In case of $\alpha = s-1$, the function $U_{s,t}(m,n,s-1,\beta)$ is non-increasing in β ($\beta \geq t-1$), while $Z_{s-1,\beta+1}(m,n)$ is clearly non-decreasing in β. Thus the maximum of the minimum of these two values in β can be found easily.*

Proof.

$$U_{s,t}(m,n,s-1,\beta) = Z_{1,t}(m-s+1,\beta) + Z_{s,t}(m-s+1,n-\beta) + (s-2)n + \beta =$$

$$(t-1)(m-s+1) + (s-2)n + \beta + Z_{s,t}(m-s+1,n-\beta).$$

By adding a vertex of degree $t-1$, we have $Z_{s,t}(m-s+1,n-\beta) \geq Z_{s,t}(m-s+1,n-(\beta+1)) + t - 1$. □

This recursion is useful in some cases. For example, Roman's bound with $p = 4$ or 5 yields $Z_{3,3}(7,7) \leq 35$. We show $Z_{3,3}(7,7) \leq 33$. (Here, in fact, equality holds.) Let $\alpha = 2$. For $\beta \leq 4$ we have $Z_{2,\beta+1}(7,7) \leq R(2,5,7,7,5) = 33$, while $U_{3,3}(7,7,2,4) = Z_{1,3}(5,4) + Z_{3,3}(5,3) + 7 + 4 = 33$. By Remark 6.2.18, we are done. Other examples that prove this recursion useful are the balanced C_4-free graphs.

PROPOSITION 6.2.19 ([C]). *Let $2 \leq q \in \mathbb{Z}$, $3-q \leq c \leq 1+q$, $c \in \mathbb{Z}$. Then*

$$Z_{2,2}(q^2+c,q^2+c) \leq (q^2+c)\left(q+\frac{1}{2}\right) + \left(\frac{c}{2}-1\right)q + \frac{c}{2} + \frac{(c-1)(c-2)}{2(q-1)}.$$

Proof. Consider the bounds in Corollary 6.2.18 with $s = t = 2$. If $\beta \leq q$, then $Z_{1,\beta+1}(q^2+c,q^2+c) \leq q(q^2+c)$, which is smaller than the bound stated provided that $c \geq 3-q$. Hence we may assume $\beta \geq q+1$. Then the second expression is $(q^2+c-1)+\beta+Z_{2,2}(q^2+c-1,q^2+c-\beta) \leq q^2+q+c+Z_{2,2}(q^2+c-1,q^2+c-q-1)$. Applying Roman's bound with $p = q-1$ to $Z_{2,2}(q^2+c-q-1,q^2+c-1)$, we get the desired result. □

REMARK 6.2.20. *It is easy to calculate that for $3-q \leq c \leq 1+q$, Roman's upper bound on $Z_{2,2}(q^2+c,q^2+c)$ gives the best result if we set $p = q$. The bound in Proposition 6.2.19 is smaller than Roman's one by*

$$\frac{q-c}{2} + \frac{(2q-c)(c-1)}{2q(q-1)}.$$

The recursive inequality of Proposition 6.2.16 can be used to achieve another bound in a more special case.

PROPOSITION 6.2.21 ([C]). *Let* $(2, v, k, 1)$ *be admissible parameters. Then*

$$Z_{2,2}(v+1, b) \leq bk + b - k(r-1).$$

Proof. Let $G = (A, B; E)$ be an extremal $K_{2,2}$-free bipartite graph of size $(v+1, b)$. Then there must be a vertex in B with degree at least $k+1$. Thus by Remark 6.2.18, we may use the transpose of Proposition 6.2.16 with $\alpha = 1$, $\beta = k+1$ to obtain

$$e(G) \leq U_{2,2}(b, v+1, 1, k+1) = (b-1) + k + 1 + Z_{2,2}(b-1, v-k).$$

Now $Z_{2,2}(b-1, v-k) \leq (v-k)r$, as deleting a block and its points from a 2-$(v, k, 1)$ design would result in a structure seen in Example 6.2.1 (so $R(2, 2, v-k, b-1, k-1) = (v-k)r$). Hence $e(G) \leq k + b + (v-k)r = bk + b - k(r-1)$. $\square$

As a corollary, we obtain that, surprisingly enough, if we add one vertex to a projective plane of order n, we cannot do anything better than the trivial extension (by one edge); however, there are different extremal constructions.

COROLLARY 6.2.22 ([C]). *Let* $2 \leq n \in \mathbb{Z}$. *Then*

$$Z_{2,2}(n^2+n+2, n^2+n+1) \leq (n^2+n+1)(n+1) + 1,$$

and equality holds if and only if a projective plane of order n exists. Moreover, any graph G reaching equality can be obtained in the following way: take a projective plane $(\mathcal{P}, \mathcal{L})$ of order n, let $A = \mathcal{P} \cup \{u_0\}$ ($u_0 \notin \mathcal{L} \cup \mathcal{P}$), $B = \mathcal{L}$. Take any vertex $v \in \mathcal{L}$, and let $\{u_1, \ldots, u_{n+1}\}$ be its neighbors in $\mathcal{P}$. Let H be any subset of the neighbors of u_1, for which $v \notin H$. Delete the edges $u_1 v'$ for all $v' \in H$, and add the edges $u_0 v$ and $u_0 v'$ for all $v' \in H$. In particular, there must be a vertex in A with degree at most $n/2 + 1$.

Proof. Proposition 6.2.21 applied to a projective plane of order n (with parameters $v = b = n^2+n+1$, $t = 2$, $\lambda = 1$, $k = n+1$) yields $Z_{2,2}(n^2+n+1, n^2+n+2) \leq (n^2+n+1)(n+1)+1$. Now let $G = (A, B)$ be a C_4-free graph on (n^2+n+2, n^2+n+1) vertices and $(n^2+n+1)(n+1)+1$ edges. Then there must be a vertex $v \in B$ of degree at least $n+2$. Consider the proof of Proposition 6.2.21. As $U_{2,2}(b, v+1, 1, k+2) = n^2+n+n+3+Z_{2,2}(n^2+n, n^2) \leq$

$n^2+2n+3+(n^2-1)(n+1) = (n^2+n)(n+1)+2 < (n^2+n+1)(n+1)+1$, v must have degree $n+2$. To reach equality, the decomposition in the proof of Proposition 6.2.16 (with $\alpha = 1$, $\beta = n+2$) assures that removing v and its neighbors $N(v) = \{u_0, \dots, u_{n+1}\}$ from G, we find an affine plane $(\mathcal{P}, \mathcal{L})$ of order n, whose points and lines correspond to $A \setminus N(v)$ and $B \setminus \{v\}$, respectively; moreover, the degree of the vertices of $B \setminus \{v\}$ in G is $n+1$. As these vertices have precisely n neighbors in $A \setminus N(v)$, each one has to be adjacent to one of the u_is. On the other hand, any u_i $(0 \leq i \leq n+1)$ may be adjacent only to the n lines of one parallel class (besides v), hence $\deg(u_i) \leq n+1$. Let $\mathcal{L}_i \subset A \setminus \{v\}$ be the parallel classes of $\mathcal{L}$ $(1 \leq i \leq n+1)$. We may assume that $N(u_i) \setminus \{v\} \subset \mathcal{L}_i$ for all $1 \leq i \leq n+1$. Let $H = N(u_0) \setminus \{v\}$; we may assume $H \subset \mathcal{L}_1$. Then $N(u_i) = \{v\} \cup \mathcal{L}_i$ for all $2 \leq i \leq n+1$, and $N(u_1) = \{v\} \cup \mathcal{L}_1 \setminus H$. Then $\deg(u_0) + \deg(u_1) = n+2$. □

Note that the gap between $Z_{2,2}(v, v)$ and $Z_{2,2}(v+1, v)$ can be arbitrarily large in general as shown by (6.3) in Corollary 6.2.15 with $c = n$ and $n+1$, n a prime power. Using the information on the lowest degree in the extremal graphs above, we obtain a slight improvement if the larger class is further extended.

PROPOSITION 6.2.23 ([C]). *Let $c \geq 1$ and $n \geq 2$, $c, n \in \mathbb{Z}$. Then*

$$Z_{2,2}(n^2+n+2+c, n^2+n+1) \leq (n^2+n+1)(n+1)+cn+1.$$

If $n \geq 3$, then

$$Z_{2,2}(n^2+n+2+c, n^2+n+1) \leq (n^2+n+1)(n+1)+cn.$$

Proof. Let $\mathcal{F}$ be the family of C_4-free bipartite graphs. The first statement follows from Proposition 6.2.22 and Theorem 6.2.9. Now suppose $n \geq 3$ and that equality holds for some $c \geq 1$, thus for $c = 1$ as well. Then any $G \in \mathrm{Ex}_{\mathcal{F}}(n^2+n+3, n^2+n+1)$ induces a graph from $\mathrm{Ex}_{\mathcal{F}}(n^2+n+2, n^2+n+1)$, which has a vertex with degree at most $n/2+1$ by Proposition 6.2.22. Deleting this vertex from G we would have $\mathrm{ex}_{\mathcal{F}}(n^2+n+2, n^2+n+1) \geq (n^2+n+1)(n+1)+n+1-(n/2+1) > (n^2+n+1)(n+1)+1$, a contradiction. □

The above bounds are sharp for $n = 2$, 3 and $c = 1$. There are ad hoc ideas that may help to determine Zarankiewicz numbers for small parameters, see Guy [43, p138]. The next proposition illustrates such a case. In the proof we rely on the fact that $Z_{2,2}(16, 16) = Z_{2,2}(15, 17) = 67$. Actually, we only need these as upper estimates. As $Z_{2,2}(8, 17) \leq R(2, 2, 8, 17, 2) = 39.5 < 5 \cdot 8$, Theorem 6.2.9

yields $Z_{2,2}(8+c,17) \leq 39+4c$. Using $Z_{2,2}(11,15) = 47$ (reported by Guy [43]), Proposition 6.2.16 yields $Z_{2,2}(16,16) \leq 67$ with $\alpha = 1$ and $\beta = 5$.

PROPOSITION 6.2.24 ([C]). $Z_{2,2}(16,17) = 70$.

Proof. Take four lines in general position in PG$(2,4)$ and take five of their six intersection points. These determine 10 flags, hence deleting these nine objects from PG$(2,4)$ we result in a C_4-free graph of size $(16,17)$ and $21\cdot5-9\cdot5+10 = 70$ edges. Now suppose to the contrary that there exists a C_4-free bipartite graph $G = (A,B;E)$ with $|A| = 16$, $|B| = 17$, $|E| = 71$. As $Z_{2,2}(16,16) = Z_{2,2}(15,17) \leq 67$, every vertex in G has degree at least four. Remark 6.2.18 yields that there can be no vertex of degree six. Hence the degree sequence of A and B are $\{4^9,5^7\}$ and $\{4^{14},5^3\}$, respectively, where the superscripts denote the multiplicity of the respective degree. Let $v \in A$, $\deg(v) = 5$, and let $N(v) = \{u_1,\dots,u_5\}$. Then $\deg(u_i) = 4$ for $1 \leq i \leq 5$, otherwise the pairwise disjoint sets $N(u_i) \setminus \{v\} \subset A \setminus \{v\}$, $1 \leq i \leq 5$, would have more than 15 elements. Let $v_i \in A$ a vertex of degree five, $1 \leq i \leq 5$. Then $|N(v_1) \cup \ldots \cup N(v_5)| \geq 5+4+3+2+1 = 15$, but there are only 14 vertices of degree four in B. $\square$

To finish this section, we give some constructions based on Baer subplanes. We may either delete or contract the points of some of them, and then delete some vertices of low degree. By the contraction of the points of a Baer subplane we mean that the point-set of a Baer subplane is replaced by one point which is incident with all the lines of the Baer subplane. Doing so, we remove $q+\sqrt{q}$ points and produce one of degree $q+\sqrt{q}+1$, so this operation is clearly better than deleting $q+\sqrt{q}$ arbitrary points. In the upcoming proposition, (2) is sharp for $q = 4$, $c = 1$ and $0 \leq h \leq 2$, and (3) is sharp for $q = 4$ and $c = 1$.

PROPOSITION 6.2.25 ([C]). *Let q be a square prime power, and let $v = q^2+q+1$, $w = q+\sqrt{q}+1$. Suppose that $1 \leq c \leq q-\sqrt{q}$, $0 \leq d \leq cw$, $0 \leq h \leq w-2$. Then*

(1) $Z_{2,2}(v-c(w-1),v-d) \geq (v-c(w-1))(q+1)+c\sqrt{q}-d(q-\sqrt{q}+2-c)$;

(2) $Z_{2,2}(v-c(w-1)-h,v) \geq (v-c(w-1)-h)(q+1)+c\sqrt{q}$;

(3) $Z_{2,2}(v-cw,v-cw) \geq (v-cw)(q+1-c)$.

Proof. Let PG$(2,q) = (\mathcal{P},\mathcal{L})$, and let $B_1 = (\mathcal{P}_1,\mathcal{L}_1),\dots,B_c = (\mathcal{P}_c,\mathcal{L}_c)$ be c pairwise disjoint Baer subplanes in it. Let $\mathcal{P}_0 = \cup_{i=1}^c \mathcal{P}_i$, $\mathcal{L}_0 = \cup_{i=1}^c \mathcal{L}_i$.

(1) Define $G = (A, B)$ in the following way. Let $A = (\mathcal{P} \setminus \mathcal{P}_0) \cup \{B_1, \dots, B_c\}$ ($|A| = v - cw + c$), $B = \mathcal{L}$. The edges between $A \cap \mathcal{P}$ and B are those defined by PG$(2, q)$; furthermore, for each $1 \le i \le c$, connect the vertex B_i to all the vertices of $\mathcal{L}_i \subset B$. (That is, we contract the points of c Baer subplanes.) As any two lines of $\mathcal{L}_i$ had an intersection in $\mathcal{P}_i$, we do not create a C_4. Note that every $\mathcal{P}_i$ is a blocking set, so every line not in $\mathcal{L}_0$ looses precisely c neighbors. The $v - cw$ vertices of $A \cap \mathcal{P}$ have degree $q+1$, the c new vertices have degree $w = q + \sqrt{q} + 1$, thus there are $(v - cw + w)(q + 1) + c\sqrt{q}$ edges in G. Let $\ell \in \mathcal{L}_i \subset \mathcal{L}_0$. Then $|\ell \cap \mathcal{P}_j|$ equals one for all $1 \le j \le c$ except for $j = i$, in which case it equals $\sqrt{q} + 1$. Hence $\deg(\ell) = q + 1 - \sqrt{q} - (c - 1)$ in G. There are $c(q + \sqrt{q} + 1)$ lines in $\mathcal{L}_0$, so we may delete any d of them to obtain a graph G' with the stated parameters.

(2) Every point of $A \cap \mathcal{P}$ has degree $q + 1$ in G, so we may delete any h of them. It is not worth deleting more than $w - 2$ points since we may contract another Baer subplane instead.

(3) Consider the graph induced by $\mathcal{P} \setminus \mathcal{P}_0$ and $\mathcal{L} \setminus \mathcal{L}_0$. Here every vertex has degree $q + 1 - c$. $\square$

6.3 Remarks

For small values of m and n, we have computed the best upper bounds one can obtain on C_4-free graphs using these ideas [C]. These values can be found in Table 1.

Illés and Krarup [49] use the formulation of Zarankiewicz's problem in terms of integer programming. They introduce Problem (R), that is, to find

$$r(n) = \max\left\{\sum_{j=1}^{n} x_j : \sum_{j=1}^{n} \binom{x_j}{2} \le \binom{n}{2}, \text{ where } x_j \ge 0, x_j \in \mathbb{Z} \text{ for all } 1 \le j \le n\right\}.$$

The cost of a solution $\mathbf{x} = (x_1, \dots, x_n)$ is $\sum_j \binom{x_j}{2}$. They call a solution $\mathbf{x}$ *realizable* if there exists an $n \times n$ $J_2 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$-free $0 - 1$ matrix in which the jth column contains x_j ones. In Remark 6, page 129 they claim: "It is conjectured that a necessary condition for realizability is that the corresponding optimal solution to (R) is a least cost solution." Note that the transpose of an optimal $n \times n$ J_2-free $0 - 1$ matrix is also an optimal matrix of that kind, hence the conjecture claims that the rows also correspond to a least cost optimal solution. As $\binom{x}{2}$ is convex, the cost of a solution to (R) is minimal if and only if $|x_i - x_j| \leq 1$ for all $1 \leq i < j \leq n$. In terms of C_4-free bipartite graphs of size (n, n), this is equivalent with saying that if such a graph has the maximum possible number of edges, then the degrees inside both classes must differ by at most one.

n \ m	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
7	**21**																
8	**22**	**24**															
9	**24**	**26**	**29**														
10	**25**	**28**	**31**	**34**													
11	**27**	**30**	**33**	**36**	**39**												
12	**28**	**32**	**36**	**39**	**42**	**45**											
13	**30**	**33**	**37**	**40**	**44**	**48**	**52**										
14	**31**	**35**	**39**	**42**	**45**	**49**	**53**	**56**									
15	**33**	**36**	**40**	**44**	**47**	**51**	**55**	**58**	**60**								
16	**34**	**38**	**42**	**46**	**50**	**53**	**57**	**60**	***64***	***67***							
17	**36**	**39**	**43**	**47**	**51**	**55**	**59**	**63**	***67***	***70***	***74***						
18	**37**	**41**	**45**	**49**	**53**	**57**	**61**	**65**	**69**	***73***	***77***	***81***					
19	**39**	**42**	**46**	**51**	**55**	**60**	**64**	**68**	**72**	***76***	***80***	***84***	***88***				
20	**40**	**44**	**48**	**52**	**57**	**61**	**66**	**70**	**75**	**80**	***84***	***88***	***92***	***96***			
21	**42**	**45**	**49**	**54**	**59**	**63**	**67**	**72**	**77**	***81***	86	***90***	***95***	***100***	**105**		
22	**43**	**47**	**51**	**55**	**60**	**65**	**69**	**73**	***78***	83	88	93	97	***101***	***106***	110	
23	**44**	**48**	**52**	**57**	**62**	**66**	**71**	**75**	***80***	85	90	95	100	105	110	113	116
24	**45**	**50**	**54**	**58**	**63**	**68**	**73**	***78***	83	88	93	98	102	107	112	117	120
25	**46**	**51**	**55**	**60**	**65**	**70**	**75**	***80***	***85***	***90***	95	100	105	110	115	120	125
26	**47**	**53**	**57**	**61**	**66**	**72**	**78**	**81**	***86***	***91***	***96***	***101***	***106***	***111***	***116***	121	126
27	**48**	**54**	**58**	**63**	**68**	**73**	**79**	**83**	***88***	***93***	***98***	***103***	***108***	***113***	***118***	***123***	***128***
28	**49**	**56**	**60**	**64**	**69**	**75**	**81**	**85**	91	***96***	***101***	***106***	***111***	***116***	***121***	***126***	***131***
29	**50**	**57**	**61**	**66**	**71**	**76**	**82**	88	93	98	103	109	***114***	***120***	***125***	***130***	***135***
30	**51**	**58**	**63**	**67**	**72**	**78**	**84**	90	95	100	105	111	117	122	127	***132***	***138***
31	**52**	**59**	**64**	**69**	**74**	**79**	**85**	91	97	102	107	113	119	125	130	135	140

TABLE 1. The table contains the best upper bounds on $Z_{2,2}(m,n)$ up to our knowledge. Bold numbers indicate equality. An exact value is in italic shape if it was not reported by Guy in [43]. In some cases we did rely on the exact values reported by Guy. Possibly undiscovered inaccuracies there may result in inaccurate values here as well.

This conjecture is false. Let $n = 8$. Then $Z_{2,2}(8, 8) = 24$. Let $G = (A, B)$ be the incidence graph of the Fano plane, and let $a \in A$ and $b \in B$ two non-adjacent vertices. Add two new vertices, u and v to A and B, respectively, and let $\{u, v\}, \{a, v\}, \{u, b\}$ be edges. The resulting graph is C_4-free, has $21 + 3 = 24$ edges, and the degrees in both classes take the values $2, 3$ and 4. However, deleting a line ℓ and a point P not on ℓ, together with all the points and lines incident with ℓ and P from $\mathrm{PG}(2, 3)$, we obtain a three-regular bipartite graph on $(8, 8)$ vertices.

We say that a vertex class of a bipartite graph is *nearly regular*, if the degrees in that class differ by at most one. We end this section by posing some questions that, to the best of our knowledge, are open. Let $2 \leq t \leq n \leq m$ be arbitrary integers.

QUESTION 6.3.1. *Does there exist an extremal $K_{t,t}$-free graph on (n, n) vertices whose classes are both nearly regular?*

QUESTION 6.3.2. *Does there exist an extremal $K_{t,t}$-free graph on (n, m) vertices with at least one nearly regular class?*

Corollary 6.2.22 shows that extremal C_4-free bipartite graphs on $(n^2 + n + 2, n^2 + n + 1)$ vertices, n a power of a prime, can not have two nearly regular classes.

It seems that if the total number of vertices is fixed in a $K_{t,t}$-free bipartite graph, then balanced graphs have the most number of edges. In fact, the known Zarankiewicz numbers satisfy $Z_{t,t}(m, n) \leq Z_{t,t}(m+1, n-1)$ whenever $m + 2 \leq n$.

QUESTION 6.3.3. *Is it true that $Z_{t,t}(n, m) \leq Z_{t,t}\left(\lfloor (n + m)/2 \rfloor, \lceil (n + m)/2 \rceil\right)$?*

Bibliography

[A] G. Araujo-Pardo, C. Balbuena, T. Héger, Finding small regular graphs of girths 6, 8 and 12 as subgraphs of cages. *Discrete Mathematics* Volume **310**, Issue 8 (2010), 1301–1306.

[B] G. Bacsó, T. Héger, T. Szőnyi, The 2-blocking number and the upper chromatic number of $\mathrm{PG}(2, q)$. *J. Comb. Des.*, accepted for publication.

[C] G. Damásdi, T. Héger, T. Szőnyi, The Zarankiewicz problem, cages and geometries. *Annales Univ. Sci. Budapest*, **56** (2013), 3–37.

[D] A. Gács, T. Héger, On geometric constructions of (k, g)-graphs. *Contrib. Discrete Math.*, **3** (2008) 63–80.

[E] A. Gács, T. Héger, Zs. Weiner, On regular graphs of girth six arising from projective planes. *European Journal of Combinatorics* **34** (2013), no. 2, 285–296.

[F] T. Héger, M. Takáts, Resolving sets and semi-resolving sets in finite projective planes. *Electronic J. Comb.* Volume **19**, Issue 4 (2012), 21 pages.

[1] M. Abreu, G. Araujo-Pardo, C. Balbuena, D. Labbate, An explicit formula for obtaining $(q + 1, 8)$-cages and others small regular graphs of girth 8. *arXiv:1111.3279v1* 14 Nov 2011.

[2] M. Abreu, M. Funk, D. Labbate, V. Napolitano, On (minimal) regular graphs of girth 6. *Australas. J. Combin.* **35** (2006), 119–132.

[3] N. Alon, L. Rónyai, T. Szabó, Norm-graphs: Variations and Applications. *Journal of Combinatorial Theory, (Series B)*, **76** (1999), 280–290.

[4] G. Araujo, D. González, J. J. Montellano-Ballesteros, O. Serra, On upper bounds and connectivity of cages. *Australas. J. Combin.* **38** (2007), 221–228.

[5] G. Araujo-Pardo, C. Balbuena, A construction of small regular graphs of girth 6. *Networks*, **57** (2011), no. 2, 121–127.

[6] G. Bacsó, Zs. Tuza, Upper chromatic number of finite projective planes. *Journal of Combinatorial Designs* **7** (2007), 39–53.

[7] R. F. Bailey, Resolving sets for incidence graphs. *Session talk at the 23rd British Combinatorial Conference*, Exeter, 5th July 2011. Slides available online at `http://www.math.uregina.ca/~bailey/talks/bcc23.pdf` (last accessed: July 12, 2013)

[8] R. F. Bailey, P. J. Cameron, Base size, metric dimension and other invariants of groups and graphs. *Bull. London Math. Soc.* **43** (2011) 209–242.

[9] R. D. Baker, Elliptic semi-planes I. Existence and classification. *Proceedings of the Eighth Southeastern Conference on Combinatorics, Graph Theory and Computing* (Louisiana State Univ., Baton Rouge, La., 1977), 61–73. Congressus Numerantium, no. XIX, Utilitas Math., Winnipeg, Man., 1977.

[10] C. Balbuena, Incidence matrices of projective planes and of some regular bipartite graphs of girth 6 with few vertices. *SIAM J. Discrete Math.* **22** (2008), no. 4, 1351–1363.

[11] C. Balbuena, P. García-Vázquez, X. Marcote, J. C. Valenzuela, Extremal $K_{(s,t)}$-free bipartite graphs. *Discrete Math. Theor. Comput. Sci.* **10** (2008), no. 3, 35–48.

[12] S. Ball, Multiple blocking sets and arcs in finite planes. *J. London Math. Soc.* **54** (1996), 581–593.

[13] S. Ball, A. Blokhuis, On the size of a double blocking set in PG(2,q). *Finite Fields Appl.*, **2** (1996) 125–137.

[14] S. Ball, A. Blokhuis, F. Mazzocca, Maximal arcs in Desarguesian planes of odd order do not exist. *Combinatorica* **17** (1997), no. 1, 31–41.

[15] S. Ball, G. Ebert, M. Lavrauw, A geometric construction of finite semifields. *J. Algebra* **311** (2007), no. 1, 117–129.

[16] S. Ball, O. Serra, Punctured combinatorial Nullstellensätze. *Combinatorica* **29** (2009), no. 5, 511–522.

[17] E. Bannai, T. Ito, On Moore graphs. *J. Fac. Sci. Uni. Tokyo Ser. A* **20** (1973), 191–208.

[18] J. Barát, S. Marcugini, F. Pambianco, T. Szőnyi, Note on disjoint blocking sets in Galois planes. *J Combin Designs* **14** (2006), no. 2, 149–158.

[19] J. Barát, L. Storme, Multiple blocking sets in PG(n,q), $n \geq 3$. *Des. Codes Cryptogr.* **33** (2004), no. 1, 5–21.

[20] L. Beukemann, K. Metsch, Regular graphs constructed from the classical generalized quadrangle $Q(4,q)$. *J. Combin. Des.* **19** (2011), Issue 1, 70–83.

[21] A. Blokhuis, A. E. Brouwer, Blocking sets in Desarguesian projective planes. *Bull. London Math. Soc.* **18** (1986), no. 2, 132–134.

[22] A. Blokhuis, L. Lovász, L. Storme, T. Szőnyi, On multiple blocking sets in Galois planes. *Advances in Geometry* **7** (2007), 39–53.

[23] A. Blokhuis, L. Storme, T. Szőnyi, Lacunary polynomials, multiple blocking sets and Baer subplanes. *J. London Math. Soc. (2)* **60** (1999), no. 2, 321–332.

[24] R. C. Bose, J. W. Freeman, D. G. Glynn, On the intersection of two Baer subplanes in a finite projective plane. *Utilitas Math.* **17** (1980), 65–77.

[25] W. G. Brown, On Hamiltonian regular graphs of girth six. *J. London Math. Soc.* **42** (1967), 514–520.

[26] R. H. Bruck, Difference sets in a finite group. *Trans. Amer. Math. Soc.* **78**, (1955), no. 2, 464–481.

[27] A. A. Bruen, Blocking sets in finite projective planes. *SIAM J. Appl. Math.* **21** (1971), 380–392.

[28] A. A. Bruen, Polynomial multiplicities over finite fields and intersection sets. *J. Combin. Theory Ser. A* **60** (1992), 19–33.

[29] B. Csajbók, Personal communication (Hungarian). *Coffee break at Combinatorics 2012, Perugia* (2012).

[30] K. Čulík, Teilweise Lösung eines verallgemeinerten Problem von K. Zarankiewicz (German). *Ann. Soc. Polon. Math.* **3** (1956), 165–168.

[31] R. M. Damerell, On Moore graphs. *Proc. Cambridge Philos. Soc.* **74** (1973), 227–236.

[32] A. A. Davydov, M. Giulietti, S. Marcugini, F. Pambianco, Linear nonbinary covering codes and saturating sets in projective spaces. *Adv. Math. Commun.* **5** (2011), no. 1, 119–147.

[33] R. H. F. Denniston, Some maximal arcs in finite projective planes. *J. Combinatorial Theory* **6** (1969) 317–319.

[34] J. M. Dover, A lower bound on blocking semiovals. *European J. Combin.* **21** (2000), 571–577.

[35] P. Erdős, H. Sachs, Reguläre Graphen gegebener Taillenweite mit minimaler Knotenzahl (German). *Wiss. Z. Uni. Halle (Math. Nat.)* **12** (1963), 251–257.

[36] G. Exoo, R. Jajcay, Dynamic cage survey. *Electr. J. Combin.* **15** (2008).

[37] W. Feit, G. Higman, The nonexistence of certain generalized polygons, *J. Algebra* **1** (1964), 114–131.

[38] S. Ferret, L. Storme, P. Sziklai, Zs. Weiner, A $t \pmod p$ result on weighted multiple $(n-k)$-blocking sets in $\mathrm{PG}(n,q)$. *Innov. Incidence Geom.* **6-7** (2009), 169–188.

[39] Z. Füredi, An upper bound on Zarankiewicz' problem. *Combinatorics, Probability and Computing* **5** (1996), 29–33.

[40] Z. Füredi, New asymptotics for bipartite Turán numbers. *Journal of Combinatorial Theory, Series A* **75** (1996), no. 1, 141–144.

[41] A. Gács, T. Szőnyi, Zs. Weiner, On the spectrum of minimal blocking sets in $\mathrm{PG}(2,q)$. Combinatorics, 2002 (Maratea). *J. Geom.* **76** (2003), no. 1–2, 256–281.

[42] J. Griggs, C. Ho, On the half-half case of the Zarankiewicz problem. *Discrete Math.* **249** (2002), no. 1–3, 95–104.

[43] R. K. Guy, The many faceted problem of Zarankiewicz in: "The Many Facets of Graph Theory". Lecture Notes in Maths **110**, Springer, (1969), 129–148.

[44] N. V. Harrach, Unique reducibility of multiple blocking sets. *J. Geometry* **103** (2012), no. 3, 445–456.

[45] T. W. Haynes, T. S. Hedetniemi, P. J. Slater, Fundamentals of domination in graphs. *Monographs and Textbooks in Pure and Applied Mathematics*, **208**. Marcel Dekker, Inc., New York (1998).

[46] J. W. P. Hirschfeld, Projective geometries over finite fields. *Clarendon Press, Oxford,* 1979, 2nd edition, 1998.

[47] A. J. Hoffman, R. R. Singleton, On Moore graphs with diameters 2 and 3. *IBM J. Res. Dev.* **4** (1960), 497–504.

[48] C. Hyltén-Cavallius, On a combinatorial problem. *Colloq. Math.* **6** (1958), 59–65.

[49] T. Illés, J. Krarup, Maximum 4-block-free matrices and knapsack-type relaxations. *PU.M.A.* **10** (1999), no. 2, 115–131.

[50] R. W. Irving, A bipartite Ramsey problem and the Zarankiewicz numbers. *Glasgow Math. J.* **19** (1978), 13–26.

[51] F. Kárteszi, Piani finiti ciclici come risoluzioni di un certo problema di minimo (Italian). *Boll. Un. Mat. Ital. (3)* **15** (1960) 522–528.

[52] F. Kárteszi, Finite Möbius planes as solutions of a combinatorial extremum problem (Hungarian). *Magyar Tud. Akad. Mat. Fiz. Oszt. Közl.* **21** (1973), 73–76.

[53] F. Kárteszi, Su certi grafi estremali (Italian). *Atti del Convegno di Geometria Combinatoria e sue Applicazioni* (Univ. Perugia, Perugia (1970)), 301–305 Ist. Mat., Univ. Perugia, Perugia, (1971).

[54] Gy. Kiss, A survey on semiovals. *Contributions to Discrete Mathematics*, **3**, no 1, 2008.

[55] T. Kővári, V. T. Sós, P. Turán, On a problem of K. Zarankiewicz. *Colloq. Math.* **3** (1954) 50–57.

[56] F. Lazebnik, V. A. Ustimenko, A. J. Woldar, New upper bounds on the order of cages. *Electron. J. Combin.* **4** (1997), no. 2, Research Paper 13, approx. 11 pp. (electronic).

[57] R. Lidl, H. Niederreiter, Finite Fields. *Cambridge University Press*, *Encyclopedia of Mathematics and Its Applications* **20** (1997).

[58] K. Metsch, On the maximum size of a maximal partial plane. *Rend. Mat. Appl.* (7) **12** (1992), no. 2, 345–355.

[59] V. Nikiforov, A contribution to the Zarankiewicz problem. *Linear Algebra Appl.* **432** (2010), no. 6, 1405–1411.

[60] S. E. Payne, J. A. Thas, Finite generalized quadrangles. Research Notes in Mathematics **110** *Pitman Advanced Publishing Program, Boston, MA* (1984) vi+312 pp.

[61] O. Polverino, Linear sets in finite projective spaces. *Discrete Math.* **310** (2010), no. 22, 3096–3107.

[62] O. Polverino, L. Storme, Unpublished manuscript (2000).

[63] I. Reiman, Über ein Problem von Zarankiewicz (German), *Acta. Math. Acad. Sci. Hungar.* **9** (1958), 269–273.

[64] I. Reiman, Su una proprietà dei 2-disegni (Italian). *Rend. Mat.* (6) **1** (1968) 75–81.

[65] S. Roman, A Problem of Zarankiewicz. *Journal of Combinatorial Theory* **18** (1975), no. 2.

[66] G. Royle, Cages of higher valency. *Web page (not updated). Available online at* `http://school.maths.uwa.edu.au/~gordon/remote/cages/allcages.html` (last accessed: April 23, 2013)

[67] L. Storme, G. Van de Voorde, Personal communication. (2012)

[68] M. Sved, Baer subspaces in the n-dimensional projective space. *Combinatorial mathematics, X* (Adelaide, 1982), 375–391, *Lecture Notes in Math.*, **1036**, Springer, Berlin, 1983.

[69] P. Sziklai, Polynomials in finite geometry. *Manuscript. Available online at* `http://www.cs.elte.hu/~sziklai/poly.html` (last accessed: July 12, 2013)

[70] T. Szőnyi, Blocking sets in Desarguesian affine and projective planes. *Finite Fields and Appl.* **3** (1997) 187–202.

[71] T. Szőnyi, Zs. Weiner, Proof of a conjecture of Metsch. *J. Combin. Theory Ser. A* **118** (2011), no. 7, 2066–2070.

[72] J. Totten, Embedding the complement of two lines in a finite projective plane, *J. Austral. Math. Soc. Ser. A* **22** (1976), no. 1, 27–34.

[73] W. T. Tutte, A family of cubical graphs. *Proc. Cambridge Philos. Soc.* **43** (1947), 459–474.

[74] G. Van de Voorde, Blocking sets in finite projective spaces and coding theory. *PhD thesis* (2010)

[75] V. I. Voloshin, Coloring Mixed Hypergraphs: Theory, Algorithms and Applications. *Amer. Math. Soc. Providence*, 2002.

[76] P. K. Wong, Cages – A survey. *J. Graph Theory* **6** (1982) 1–22.

[77] K. Zarankiewicz, Problem of P101. *Colloq. Math.*, **2** (1951), p. 301.

Acknowledgements

First of all I am most grateful to my supervisors, András Gács and Tamás Szőnyi. The lecture on symmetric structures András held in 2006 was so enjoyable that I decided to write my master's thesis under his supervision, which happened to be a really good idea. However, the topic of that thesis was due to Tamás Szőnyi, as he mined out a fresh paper on $(k, 6)$-graphs from his handbag and gave it to András to see if we can make use of it. Although we did make progress in the research, I would have never thought of applying for a PhD grant if András had not encouraged me to do so. I was very proud when, for the first time, I could prove something with polynomials on my own – and I was very sad that I could not show it to András. His tragic, unexpected death in the autumn of 2009 was a great loss for mathematics and for many of us who had known him personally. Since then my supervisor has been Tamás Szőnyi, whom I owe a large debt to. His wide and deep knowledge on finite geometrical literature was an excellent source I could always turn to learn from, and his ideas were clear guidelines in my research. I am also heavily thankful for his incredible solicitousness for the mathematical career of many, including myself. His stable, reliable support has made my life a lot easier. I also wish to express my gratitude to László Lovász, who had supported my research for almost three years. My work was funded by ERC Grant 227701 DISCRETECONT, and by the Hungarian National Foundation for Scientific Research (OTKA) grants T 67867 and K 81310.

Besides András and Tamás, I am also greatly thankful to Péter Sziklai, who had never been too busy to answer my questions and share his valuable insights.

Special thanks go to my coauthors, Gabriela Araujo–Pardo, Gábor Bacsó, Camino Balbuena, Gábor Damásdi, Marcella Takáts, and Zsuzsa Weiner for the fruitful collaboration.

Thank you Gábor Bacsó and Marcella Takáts for proofreading this thesis and the extended abstract, respectively.

I thank Marcella Takáts, my roommate at ELTE, for being such good company, improving my Hungarian grammar, bringing so much delicious cakes and various kinds of chocolate, and for so carefully observing the occupational health-care directives.

Finally, I am very much grateful to my parents for their constant support and care.

Appendix

Proof of the Szőnyi–Weiner Lemma

Here we give the proof of the Szőnyi–Weiner Lemma which has proved quite useful in finite geometry. It was developed by Szőnyi and Weiner in [A-2, A-3, A-4]. The proof given here is entirely based on Sziklai's monograph [A-1, Section 9.5, pp54–59], which is in preparation at the present time; there one finds all elements needed. However, the structure and the formulation of the current proof is slightly different from the mentioned versions.

Let us introduce some notation and assumptions that will be valid in the sequel. Let $f(X) = \sum_{i=0}^{k} a_i X^{k-i}$, $g(X) = \sum_{i=0}^{l} b_i X^{l-i}$, $f, g \in \mathbb{F}[X]$, $\mathbb{F}$ an arbitrary field, where $a_0 \neq 0$ or $b_0 \neq 0$. Let $r(X) = \gcd(f(X), g(X))$ with leading coefficient equal to one (i. e., r is monic), and let $\deg r(X) = \mu$. Let $m \in \mathbb{Z}$, $m \geq 0$, $m \leq \min\{k, l\}$. The polynomials $\overline{c} = \sum_{i=0}^{k-m} c_i X^{k-m-i}$ and $\overline{d} = \sum_{i=0}^{l-m} d_i X^{l-m-i}$ are supposed to satisfy $c_0 = a_0$, $d_0 = b_0$, and they are regarded as unknowns. Coefficients "out of range" are considered to be zero. Let

$$R_m(f,g) = \left(\begin{array}{cccc|cccc} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ \vdots & \vdots & \ddots & & \vdots & \vdots & \ddots & \\ a_{l-m-1} & \vdots & & a_0 & b_{l-m-1} & \vdots & & b_0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{k+l-2m-1} & \cdots & \cdots & a_{k-m} & b_{k+l-2m-1} & \cdots & \cdots & b_{l-m} \end{array} \right) .$$
$$\underbrace{\qquad\qquad\qquad\qquad}_{l-m} \qquad \underbrace{\qquad\qquad\qquad\qquad}_{k-m}$$

Note that $R_m(f,g) \in \mathbb{F}^{k+l-2m \times k+l-2m}$, $R_0(f,g)$ is the Sylvester-matrix of f and g, and $\det(R_0(f,g))$ is the resultant of f and g.

Consider the following polynomial equation (with unknowns $\overline{c}$ and $\overline{d}$).

$$\overline{d}f - \overline{c}g = 0 \qquad \text{(A-1)}$$

Proposition 1. *Let $m \leq \mu$. Then the set of solutions of* (A-1) *form a* $(\mu - m)$ *dimensional vector space over* $\mathbb{F}$.

Proof. We may assume that neither f or g is the zero polynomial, otherwise the assertion is trivial. Suppose that $\overline{c}$, $\overline{d}$ form a solution of (A-1). By $f \mid \overline{c}g$, it is clear that $\overline{c} = \frac{f}{r}\overline{u}$, and similarly, $\overline{d} = \frac{g}{r}\overline{v}$ for some $\overline{u}, \overline{v} \in \mathbb{F}[x]$. Then $\overline{u} = \overline{v}$ follows immediately from $\frac{fg}{r}\overline{u} = \frac{fg}{r}\overline{v}$. As, say, $c_0 = a_0 \neq 0$, $\overline{c} = \frac{f}{r}\overline{u}$ (or $\overline{d} = \frac{g}{r}\overline{u}$) implies that $\overline{u} \in \mathbb{F}[X]$ is monic, and it has degree precisely $\mu - m$. □

Proposition 2. *Suppose that $m \leq \mu$. Then the rank of the matrix $R_m(f, g)$ is $k + l - 2m - (\mu - m)$.*

Proof. As $\deg r = \mu \geq m$ and r divides $\overline{d}f - \overline{c}g$, $\overline{c}$ and $\overline{d}$ form a solution of (A-1) if and only if $\deg(\overline{d}f - \overline{c}g) < m$. As

$$\begin{aligned}&\overline{d}f - \overline{c}g = \\ &\quad \sum_{i=0}^{l-m} d_i X^{l-m-i} \sum_{j=0}^{k} a_j X^{k-j} - \sum_{i=0}^{k-m} c_i X^{k-m-i} \sum_{j=0}^{k} b_j X^{l-j} = \\ &\quad \sum_{i=0}^{k+l-m} \left(\sum_{j=0}^{i} d_j a_{i-j} - c_j b_{i-j} \right) X^{k+l-m-i},\end{aligned}$$

this is equivalent to $\sum_{j=0}^{i} d_j a_{i-j} - c_j b_{i-j} = 0$ for all $0 \leq i \leq k + l - 2m$. Now consider $R_m(f, g)(d_1, \ldots, d_{l-m}, -c_1, \ldots, -c_{k-m})^T$. The ith coordinate of this vector is $\sum_{j=1}^{i}(d_j a_{i-j} - c_j b_{i-j})$. Recall that $c_0 = a_0$ and $d_0 = b_0$. Hence $\sum_{j=0}^{i} d_j a_{i-j} - c_j b_{i-j} = 0$ for all $0 \leq i \leq k + l - 2m$ if and only if

$$\begin{aligned}&R_m(f, g)(d_1, \ldots, d_{l-m}, -c_1, \ldots, -c_{k-m})^T = \\ &\quad (a_0 b_1 - a_1 b_0, \ldots, a_0 b_{k+l-2m} - a_{k+l-2m} b_0)^T. \qquad \text{(A-2)}\end{aligned}$$

By Proposition 1, the solutions (A-1), and hence those of (A-2) form a subspace of dimension $\mu - m$, which is the dimension of the kernel of $R_m(f, g)$. □

A unique factorization domain (UFD) is a commutative ring in which every non-zero non-unit element can be written as a product of irreducible elements, uniquely up to the order of the elements and unit multipliers. Polynomial rings in any number of variables over a field are UFDs.

Lemma 3 (Sziklai). *Let $M \in R^{n \times n}$, R a unique factorization domain. Suppose that all $(n-1) \times (n-1)$ subdeterminants of M are divisible by r^s, $r \in R$, $1 \leq s \in \mathbb{N}$. Then r^{s+1} divides* $\det(M)$.

Proof. Let $M^* \in R^{n\times n}$ be the matrix where $(M^*)_{i,j}$ is the signed $(n-1)\times(n-1)$ subdeterminant of M corresponding to the position (j,i). By our assumption, r^s divides all entries of M^*, therefore r^{sn} divides $\det(M^*)$. On the other hand, $M^*M = \det(M)I_n$, hence $\det(M^*)\det(M) = \det(M)^n$, thus $r^{sn} \mid \det(M^*) = \det M^{n-1}$, and the assertion follows. □

From now on let $a_i = a_i(Y)$ and $b_i = b_i(Y)$ be polynomials of degree $\deg a_i \le i$, $\deg b_i \le i$. (In other words, $f, g \in \mathbb{F}[X,Y]$ of total degree at most k and l, respectively, and also $f, g \in F[X]$, where $F = \mathbb{F}(Y)$ is the field of rational expressions over F in the indeterminate Y). Then every entry of $R_m(f,g) = R_m(Y)$ and hence $\det(R_m(Y))$ is a polynomial in Y. Recall $a_0 \ne 0$ or $b_0 \ne 0$.

PROPOSITION 4. *Fix $y \in \mathbb{F}$. Let $r(X) = \gcd(f(X,y), g(X,y))$, $\deg(r) = \mu \ge m$. Then $(Y-y)^{\mu-m} \mid \det(R_m(Y))$.*

Proof. By Proposition 2 we have that all $(k+l-2m-(\mu-m)+1)\times(k+l-2m-(\mu-m)+1)$ subdeterminants of $R_m(y)$ are zero, hence $(Y-y)$ divides all such subdeterminants of $R_m(Y)$. Iterating Lemma 3 finishes the proof. □

PROPOSITION 5. *Let $m \le \mu$. Then* $\deg\det R_m(Y) \le (k-m)(l-m)$.

Proof. $(R_m(Y))_{i,j}$ has degree at most $i-j$ if $j \le l-m$, and at most $i-j+(l-m)$ otherwise. Hence for any permutation $\pi : \{1,\dots,k+l-2m\} \to \{1,\dots,k+l-2m\}$ we have $\deg\left(\prod_{i=1}^{k+l-2m}(R_m(Y))_{i,\pi(i)}\right) \le \sum_{i=1}^{k+l-2m}(i-\pi(i)) + (k-m)(l-m) = (k-m)(l-m)$, hence the assertion follows. □

In the upcoming formulation of the Szőnyi–Weiner Lemma, all necessary assumptions are included. If the field $\mathbb{F}$ is not finite, then the sum ranges over the finitely many nonzero addends. For $\alpha \in \mathbb{Z}$, let $\alpha^+ = \max\{0,\alpha\}$.

RESULT 6 (Szőnyi–Weiner Lemma). *Let $f, g \in \mathbb{F}[X,Y]$, where $\mathbb{F}$ is an arbitrary field, and suppose that the coefficient of the term $X^{\deg f}$ in f is nonzero. Let $k_y = \deg\gcd(f(X,y), g(X,y))$, $y_0 \in \mathbb{F}$ arbitrary. Then*

$$\sum_{y\in F}(k_y - k_{y_0})^+ \le (\deg f(X,Y) - k_{y_0})(\deg g(X,Y) - k_{y_0}).$$

Proof. Let $m = k_{y_0}$. Then $\det R_m(y_0) \ne 0$ by Proposition 2, hence $\det R_m(Y) \not\equiv 0$. Applying Proposition 4 we get that for all $y \in \mathbb{F}$, $(Y-y)^{(k_y-m)^+}$ divides $R_m(Y)$, which has degree at most $(\deg f - m)(\deg g - m)$ by Proposition 5. □

Bibliography

[A-1] P. Sziklai, Polynomials in finite geometry. *Manuscript. Available online at* `http://www.cs.elte.hu/~sziklai/poly.html` (last accessed: July 12, 2013)

[A-2] T. Szőnyi, On the embedding of (k, p)-arcs. *Des. Codes Cryptogr.* **18** (1999) 235–246.

[A-3] Zs. Weiner, On (k, p^e)-arcs in Galois planes of order p^h. *Finite Fields Appl.* **10** (2004) 390–404.

[A-4] T. Szőnyi, Zs. Weiner, Proof of a conjecture of Metsch. *J. Combin. Theory Ser. A* **118** (2011), no. 7, 2066–2070.

Summary

The thesis treats problems in finite geometry that either try to answer graph theoretical questions, or originate from graph theory. However, the emphasis is on the finite geometrical viewpoint. In some problems we use the polynomial method (Rédei-polynomials, the Szőnyi–Weiner Lemma, and the combinatorial Nullstellensatz with multiplicities).

In Chapter 2 we collect results on multiple blocking sets, which are closely related to three of the four main problems. We show that through any essential point of a t-fold blocking set of size $t(q+1)+k$ in $\mathrm{PG}(2,q)$ there pass at least $q+1-k-t$ distinct t-secants. If q is not a square, no general construction for small t-fold blocking sets were known if $t \geq 2$. We construct a small double blocking set in $\mathrm{PG}(2,q)$ for each $q = p^h$, where p and $h \geq 3$ are odd.

The classical problem of (k,g)-cages asks for the order of the smallest k-regular graph of girth g. For $n = 3,4,6$, $(q+1, 2n)$ cages are the incidence graphs of generalized n-gons of order q. In Chapter 3 we study the regular subgraphs of these extremal graphs. We characterize all $(q+1-t)$-regular induced subgraphs of the incidence graph of $\mathrm{PG}(2,q)$, $q = p^h$, if $t \leq p$ and $t \leq \sqrt{q}/2$ (roughly), and also construct some induced and non-induced regular subgraphs for $n = 4,6$.

In Chapter 4 we show that any small semi-resolving set for $\mathrm{PG}(2,q)$ can be extended to a double blocking set by adding at most two points to it. As a corollary, we obtain a new lower bound on the size of blocking semiovals.

The upper chromatic number of $\mathrm{PG}(2,q)$, considered as a hypergraph, is proved to equal $q^2+q+2-\tau_2(\mathrm{PG}(2,q))$ in Chapter 5, provided that $q > 256$ is a square or $q = p^h$, $p \geq 29$ and $h \geq 3$ is odd. In addition, we show that the coloring reaching this bound is essentially unique.

We treat the Zarankiewicz problem in Chapter 6, focusing on the case of C_4-free bipartite graphs. We provide exact values for several sets of the parameters, and also exhibit a table of exact values for small parameters.

Összefoglaló

A tézis olyan véges geometriai kérdésekkel foglalkozik, melyek vagy gráfelméleti problémákra keresnek megoldást, vagy gráfelméleti ihletésűek; a hangsúly mindazonáltal a véges geometriai megközelítésen van. A bizonyítások során olykor a polinomos módszerre támaszkodunk (Rédei polinomok, Szőnyi–Weiner-lemma, kombinatorikus nullhelytétel multiplicitásos változata).

A 2. fejezetben többszörös lefogó ponthalmazokat vizsgálunk. Ezek a dolgozat négy fő kérdéséből hárommal szoros kapcsolatban állnak. Megmutatjuk, hogy egy $\mathrm{PG}(2,q)$-beli, $t(q+1)+k$ pontú, t-szeres lefogó ponthalmaz minden lényeges pontján át legalább $q+1-k-t$ darab t-szelő halad. Kicsi többszörös lefogó ponthalmazokra nem volt általános konstrukció, ha q nem négyzetszám; mi adunk egyet kétszeres lefogókra, ha p és h páratlanok, ahol $q=p^h$, $h \geq 3$.

Egy klasszikus gráfelméleti probléma a legkisebb k-reguláris, g bőségű gráfok csúcsszámának meghatározása. Ha $n=3,4,6$, akkor a legkisebb $(q+1,2n)$-gráfok az általánosított $2n$-szögek illeszkedési gráfjai. A 3. fejezetben ezen extrém példák reguláris részgráfjait vizsgáljuk. Leírjuk a $\mathrm{PG}(2,q)$, $q=p^h$, illeszkedési gráfjának az összes $(q+1-t)$-reguláris feszített részgráfját, közelítőleg a $t \leq p$ és $t \leq \sqrt{q}/2$ feltételek mellett, továbbá adunk konstrukciókat az $n=4,6$ esetekben is.

A 4. fejezetben megmutatjuk, hogy $\mathrm{PG}(2,q)$ minden kicsi féligmegoldó-halmaza előáll egy kétszeres lefogó ponthalmazból legföljebb két pont elhagyásával. Ebből nyerünk egy alsó korlátot blokkoló szemioválisok méretére is.

A $\mathrm{PG}(2,q)$ sík mint hipergráf fölső kromatikus száma $q^2+q+2-\tau_2(\mathrm{PG}(2,q))$ az 5. fejezet tanúsága szerint, feltéve, hogy $q>256$ egy négyzetszám, vagy $q=p^h$, $p \geq 29$ prím és $h \geq 3$ páratlan. Ráadásként az is kiderül, hogy lényegében egyetlen színezés éri el ezt a korlátot.

A 6. fejezetben Zarankiewicz problémájával, és azon belül kiemelten a C_4-mentes páros gráfokkal foglalkozunk. Meghatározunk pontos értékeket bizonyos paramétertartományokban, és egy táblázatban közreadunk kis paraméterekre vonatkozó pontos értékeket is.