Blocking and double blocking sets in finite planes

Jan De Beule[*]

Vrije Universiteit Brussel
Department of Mathematics
Pleinlaan 2, B–1050 Brussels, Belgium

jan@debeule.eu

Tamás Héger

MTA–ELTE Geometric and Algebraic Combinatorics Research Group
Eötvös Loránd University
1117 Budapest, Pázmány Péter sétány 1/C, Hungary

hetamas@cs.elte.hu

Tamás Szőnyi[†]

Department of Computer Science and
MTA–ELTE Geometric and Algebraic Combinatorics Research Group
Eötvös Loránd University
1117 Budapest, Pázmány Péter sétány 1/C, Hungary

szonyi@cs.elte.hu

Geertrui Van de Voorde[‡]

Ghent University
Department of Mathematics
Krijgslaan 281, S22, B–9000 Gent, Belgium

gvdvoorde@cage.ugent.be

Submitted: Nov 17, 2015; Accepted: Mar 17, 2016; Published: Apr 1, 2016
Mathematics Subject Classifications: 51E21, 05B25, 11T06

Abstract

In this paper, by using properties of Baer subplanes, we describe the construction of a minimal blocking set in the Hall plane of order q^2 of size $q^2 + 2q + 2$ admitting

[*]This author has been supported as a postdoctoral fellow of the Research Foundation Flanders (Belgium) (FWO).

[†]This author was supported by a Visiting Professor grant of the Special Research Fund - Ghent University (BOF project number 01T00413) and a Research Grant of the Research Foundation Flanders (Belgium) (FWO) (project number 1504514N).

[‡]This author is a postdoctoral fellow of the Research Foundation Flanders (Belgium) (FWO).

1-,2-,3-,4-, $(q+1)$- and $(q+2)$-secants. As a corollary, we obtain the existence of a minimal blocking set of a non-Desarguesian affine plane of order q^2 of size at most $4q^2/3+5q/3$, which is considerably smaller than $2q^2-1$, the Jamison bound for the size of a minimal blocking set in an affine Desarguesian plane of order q^2.

We also consider particular André planes of order q, where q is a power of the prime p, and give a construction of a small minimal blocking set which admits a secant line not meeting the blocking set in 1 mod p points. Furthermore, we elaborate on the connection of this problem with the study of value sets of certain polynomials and with the construction of small double blocking sets in Desarguesian projective planes; in both topics we provide some new results.

Keywords: minimal blocking set, Baer subplane, stabiliser of a Baer subplane, Hall plane, André plane, double blocking set, value set of polynomials.

1 Introduction

In finite geometry one often studies combinatorial analogues of classical substructures of Galois geometries. In case of projective planes, examples of such combinatorially defined substructures are arcs, ovals and hyperovals, (k,n)-arcs, unitals, blocking sets and multiple blocking sets. Most results regarding these are for planes coordinatized over finite fields (i.e. Desarguesian planes) and are obtained by using algebraic methods. Therefore it is an interesting question to decide whether these results remain valid for non-Desarguesian planes or not. It is not too surprising that only few results have a combinatorial proof, and in most cases one can find counterexamples showing that the strong results for Desarguesian planes cannot be extended to non-Desarguesian ones. One strategy for constructing counterexamples is to consider a substructure of a Desarguesian plane and study when this subset will be a similar inherited substructure in a suitable non-Desarguesian plane. Another strategy for constructing examples and counterexamples is to use higher-dimensional representations of non-Desarguesian planes (the André/Bruck–Bose representation). These methods can be successful and the present paper illustrates both of them but the focus is on the first one. The early results on inherited substructures were about ovals, the reader is referred to [18]. More recent results in this direction can be found in [17]. In the present paper we use inherited substructures for constructing blocking sets in Hall- and André planes.

1.1 Preliminaries

A *blocking set* $\mathcal{B}$ in a projective plane Π_q of order q is a set of points such that every line of Π_q contains at least one point of $\mathcal{B}$. We also say that the set $\mathcal{B}$ *blocks* all lines. A *minimal* blocking set $\mathcal{B}$ is a blocking set such that no proper subset of $\mathcal{B}$ is a blocking set. An *essential point* of a blocking set is a point lying on at least one tangent line to $\mathcal{B}$ and we see that $\mathcal{B}$ is minimal if and only if every point of $\mathcal{B}$ is essential. A blocking set is called *trivial* if it contains a line. A *t-fold* blocking set is a set of points such that every line contains at least t points of $\mathcal{B}$. A 1-fold blocking set is simply a blocking set and a

2-fold blocking set is mostly called a *double blocking set.* A *Baer subplane* of an arbitrary projective plane of order q^2, is a set of q^2+q+1 points such that its inherited point-line structure forms a projective subplane of order q. It is well-known that any Baer subplane is a blocking set in its ambient plane.

A blocking set $\mathcal{B}$ in a projective plane of order q is said to be *of Rédei type* if there exists a line ℓ such that $|\mathcal{B}| = q + |\mathcal{B} \cap \ell|$. Given a set $\mathcal{U}$ of q points in an affine plane, the set of *determined directions* is the set $\mathcal{D}_{\mathcal{U}}$ of those points on the line at infinity that admit a line through them which intersects $\mathcal{U}$ in at least two points. It is well-known that $\mathcal{U} \cup \mathcal{D}_{\mathcal{U}}$ is a blocking set of Rédei type in the projective closure. For more details, we refer to [20].

Let us first collect some results on blocking sets in Desarguesian planes. We denote by $\mathrm{PG}(2,q)$ and $\mathrm{AG}(2,q)$ the projective and affine plane over the q-element field $\mathrm{GF}(q)$.

Result 1.1 (Szőnyi [19])**.** *Let $q = p^h$, p prime, $h \geqslant 1$, and let $\mathcal{B}$ be a minimal blocking set in* $\mathrm{PG}(2,q)$ *of size less than* $\frac{3}{2}(q+1)$. *Then every line intersects $\mathcal{B}$ in* $1 \pmod p$ *points.*

Result 1.2 (Blokhuis–Storme–Szőnyi [4])**.** *Let $\mathcal{B}$ be a t-fold blocking set in* $\mathrm{PG}(2,q)$, *$q = p^h$, p prime, of size $t(q+1)+C$. Let $c_2 = c_3 = 2^{-1/3}$ and $c_p = 1$ for $p > 3$.*
(1) If $q = p^{2d+1}$ and $t < q/2 - c_p q^{2/3}/2$, then $C \geqslant c_p q^{2/3}$;
(2) if q is a square, $t < \min\{q^{1/4}/2, c_p q^{1/6}\}$, and $C < c_p q^{2/3}$, then $\mathcal{B}$ contains the union of t disjoint Baer subplanes.

Result 1.3 (Jamison [13], Brouwer–Schrijver [5])**.** *A blocking set of* $\mathrm{AG}(2,q)$ *has at least* $2q-1$ *points.*

If $\mathcal{B}$ is a blocking set in a projective plane Π and on a point $P \in \mathcal{B}$ there are t tangents to $\mathcal{B}$, we may take one point on each but one, say, ℓ, of these tangents, add these points to $\mathcal{B}$ and remove P from $\mathcal{B}$ to obtain a blocking set in the affine plane $\Pi \setminus \ell$ of size $|\mathcal{B}|+t-2$. This well-known idea shows that Result 1.3 is equivalent with the following.

Result 1.4. *Let $\mathcal{B}$ be a blocking set in* $\mathrm{PG}(2,q)$. *Then each essential point of $\mathcal{B}$ lies on at least* $2q - |\mathcal{B}| + 1$ *tangent lines to $\mathcal{B}$.*

After the third author's talk at the 37th ACCMCC, Gordon Royle asked whether the 1 modulo p result (Result 1.1) for blocking sets in Galois planes could be extended for non-Desarguesian planes. In a sense this question was the starting point for this paper.

In Section 3, we provide information about Baer subplanes of Desarguesian projective planes and their stabilisers which will be applied in Hall planes. In Section 4, we construct small blocking sets in non-Desarguesian planes and show that, as expected, the above mentioned results on blocking sets do not hold for non-Desarguesian planes in general. These results are also related to small double blocking sets in Desarguesian planes. Let us state some of our results here.

Theorem 1.5. *Let $q^2 \geqslant 9$ be a square prime power. Then in the Hall plane of order q^2 there is a minimal blocking set of size q^2+2q+2 admitting* 1-, 2-, 3-, 4-, $(q+1)$- *and* $(q+2)$-*secants.*

Theorem 1.6. *Let $q^2 \geqslant 9$ be a square prime power. Then there exists an affine plane of order q^2 in which there is a blocking set of size $\lfloor 4q^2/3 + 5q/3 \rfloor$.*

Note that regarding Result 1.3, there was one counterexample known: Bruen and de Resmini ([6], 1983) constructed a blocking set of size 16 in a particular non-Desarguesian affine plane of order 9. However, Bierbrauer [3] pointed out that the construction works in all non-Desarguesian affine planes of order 9.

Theorem 1.7. *Let* $\mathrm{GF}(r)$ *be a proper subfield of* $\mathrm{GF}(q)$*, and suppose that* $\gcd(r-2, q-1) = 1$*,* $r \geqslant 4$*. Then there exists a projective plane of order q in which there is a minimal blocking set of size $q + 2(q-1)/(r-1)$ admitting an $r+2$-secant.*

Theorem 1.8. *Let $\mathcal{B}$ be a non-trivial blocking set in* $\mathrm{PG}(2, p^h)$*, p prime, $h \geqslant 2$, of size $|\mathcal{B}| \leqslant \frac{3}{2}(p^h - p^{h-1})$. Then there exists a blocking set of size $p^h + p^{h-1} + 1$ that is disjoint from $\mathcal{B}$. Consequently, if $p > 5$, then there exists a double blocking set in* $\mathrm{PG}(2, p^h)$ *of size $2(p^h + p^{h-1} + 1)$.*

Additionally, we apply the same methods to find small double blocking sets with respect to k-spaces in $\mathrm{PG}(2k, p^h)$.

In Section 2, we show some connections of the above results with value sets of certain polynomials. For a polynomial $f \in \mathrm{GF}(q)[x]$, let $V(f) = \{f(x) \colon x \in \mathrm{GF}(q)\}$ denote the value set of f. As usual, we consider x^{-a} and x^{q-1-a} as the same functions, and thus we interpret 0^{-a} as zero. Determining the size of the value set of polynomials is hard in general. Cusick [7] and, based on Cusick's work, Rosendahl [16] examined the value sets of polynomials of the form $s_a(x) = x^a(x+1)^{\sqrt{q}-1}$, q a square, and have derived several exact results, mostly in the case when q is even. Their proofs depend on the arithmetic of $\mathrm{GF}(q)$ and connections to cross-correlation functions. If q is odd, then, up to our knowledge, the following are the only known corresponding results. Note that one may define these polynomials more generally with respect to any field extension $\mathrm{GF}(q) \subset \mathrm{GF}(q^h)$ as

$$s_a(x) = x^a(x+1)^{q-1}.$$

Result 1.9 (Cusick–Müller [8])**.** *For any prime power q and $h \geqslant 2$, the size of the value set of $s_1(x) = x(x+1)^{q-1}$ in* $\mathrm{GF}(q^h)$ *is*

$$|V(s_1)| = (1 - 1/q)q^h.$$

Result 1.10 (Rosendal [16])**.** *Assume that $q \equiv 0 \pmod 3$. Then the size of the value set of $s_3(x) = x^3(x+1)^{q-1}$ in* $\mathrm{GF}(q^2)$ *is*

$$|V(s_3)| = \frac{2}{3}q^2 - \frac{1}{6}q - \frac{1}{2}.$$

Let us remark that [16, Theorem 2.8] states the above formula for $q \equiv 1 \pmod 3$, q odd as well but, a short check using GAP [10] shows that the result actually fails in that case. Using the connections to be established in Section 2, in Section 5 we obtain the following result.

Theorem 1.11. *Let q be odd. The size of the value set of $s_{-1}(x) = x^{-1}(x+1)^{q-1}$ in* $\mathrm{GF}(q^2)$ *is*

$$|V(s_{-1})| = \begin{cases} \frac{2}{3}q^2 - \frac{1}{6}q - \frac{1}{2} & \text{if } q \not\equiv 2 \pmod 3, \\ \\ \frac{2}{3}q^2 - \frac{1}{6}q + \frac{1}{6} & \text{if } q \equiv 2 \pmod 3. \end{cases}$$

Let us remark that our methods work for q even as well, for which case the respective results have already been obtained by Cusick [7] and Rosendahl [16], see Section 5.

2 Connections of double blocking sets of $\mathbf{PG(2, q^h)}$, lines of André planes, and value sets of certain polynomials

In the following, unless stated otherwise, q denotes an arbitrary power of a prime p, and we consider $\mathrm{GF}(q^h)$, $h \geqslant 2$ as the extension of $\mathrm{GF}(q)$. For a field $\mathcal{F}$, $\mathcal{F}^*$ denotes its multiplicative group. We use $(x : y : z)$ to denote a homogeneous triplet over the respective field. We call $\ell_\infty = \{(1 : y : 0) \colon y \in \mathrm{GF}(q^h)\} \cup \{(0 : 1 : 0)\}$ the line at infinity of $\mathrm{PG}(2, q^h)$, and we let $\mathrm{AG}(2, q^h)$ denote the affine plane $\mathrm{PG}(2, q^h) \setminus \ell_\infty$. Recall that $x \mapsto x^q$ is an automorphism of $\mathrm{GF}(q^h)$.

Let $D = \{x^{q-1} \colon x \in \mathrm{GF}(q^h)^*\}$ be the set of $(q-1)$-th powers in $\mathrm{GF}(q^h)^*$, and let $\mathcal{D} = \{(1 : s : 0) \colon s \in D\} \subset \ell_\infty \in \mathrm{PG}(2, q^h)$ be the set of common points of lines with slope in D. We define $k := \gcd(q-2, q^h-1) = \gcd(q-2, 2^h-1)$ and $C := \{x^{q-2} \colon x \in \mathrm{GF}(q^h)^*\} = \{x^k \colon x \in \mathrm{GF}(q^h)^*\}$.

We consider the following model for a particular affine André plane of order q^h. The upcoming method for constructing projective planes, due to T. G. Ostrom for $h = 2$, is called derivation. For more information on derivation and derived planes, we refer to [12]. We use $\mathcal{D}$ as a derivation set, that is, for all $a \in D$, we replace the lines of $\mathrm{AG}(2, q^h)$ with equation $y = ax + b$ by other suitable subsets, namely those defined by the equation $y = ax^q + b$. For our purposes, it will be convenient to introduce the following notation.

$$f_{a,c}(x) := ax^q - ac, \text{ where } a \neq 0.$$

As $(f_{a,c}(x) - f_{a,c}(y))/(x-y) = (ax^q - ay^q)/(x-y) = a(x-y)^{q-1}$, the directions determined by (the graph of) $f_{a,c}$ are $\{ax^{q-1} \colon x \in \mathrm{GF}(q^h)^*\}$, which correspond to the points $\{(1 : ax^{q-1} : 0) \colon x \neq 0\} = \{(1 : s : 0) \colon s \in aD\} =: \mathcal{D}(a)$ on the line at infinity. Hence, the following sets are blocking sets of Rédei type in $\mathrm{PG}(2, q^h)$:

$$\mathcal{B}(a,c) = \underbrace{\{(x : f_{a,c}(x) : 1) : x \in \mathrm{GF}(q^h)\}}_{\mathcal{U}(a,c)} \cup \underbrace{\{(1 : ax^{q-1} : 0) : x \in GF(q^h)^*\}}_{\mathcal{D}(a)}.$$

Then an affine André plane can be constructed in the following way. Define the set $\mathcal{P}$ as the set of points of $\mathrm{AG}(2, q^h)$. Define the set $\mathcal{L}$ as a set of lines of two types:

(i) the lines of $\mathrm{PG}(2, q^h)$ meeting ℓ_∞ not in $\mathcal{D}$;

(ii) the sets $\mathcal{B}(a,c)$, where $a \in D$, $c \in \mathrm{GF}(q^h)$.

The incidence I is the natural incidence. It is well known that $\Pi^A_{\mathcal{D}} := (\mathcal{P}, \mathcal{L}, \mathrm{I})$ is an affine plane of order q^h (and it is easy to check as well). Its projective completion $\Pi_{\mathcal{D}}$ is a projective André plane of order q^h. Unless causing confusion, we write simply Π and Π^A instead of $\Pi_{\mathcal{D}}$ and $\Pi^A_{\mathcal{D}}$. It is clear that the parallel classes of lines of type (ii) are the sets $[a] := \{\mathcal{B}(a,c) \colon c \in \mathrm{GF}(q^h)\}$, where $a \in D$, as $\mathcal{U}(a,c_1)$ and $\mathcal{U}(a,c_2)$ are disjoint if $c_1 \neq c_2$. For each $a \in D$, let (a) denote the common point of the lines of $[a]$, and let $\mathcal{D}' = \{(a) \colon a \in D\}$. The points of $\ell_\infty \setminus \mathcal{D} \subseteq \mathrm{PG}(2,q^h)$ naturally correspond to the common points of the parrallel classes of lines of type (i) in Π^A. Note that the point set of a line $\mathcal{B}(a,c)$ of type (ii) in Π is $\mathcal{U}(a,c) \cup \{(a)\}$. The directions in $\mathcal{D}'$ and lines of type (ii) are also called derived directions and derived lines, respectively.

We will denote by ℓ'_∞ the line at infinity in $\Pi_{\mathcal{D}}$. In what follows, we will often consider an object in one plane (Π or $\mathrm{PG}(2,q^2)$), and interpret it in the other plane, e.g., a line of type (ii) in Π is a blocking set of $\mathrm{PG}(2,q^2)$, an affine point of $\mathrm{PG}(2,q^2)$ is an affine point of Π, etc. Note that if $h = 2$, then $\mathcal{B}(a,c)$ is always a Baer subplane, and the plane Π is the well known Hall plane of order q^2. In this case, the set of all lines of type (ii) in Π is the set of all Baer subplanes in $\mathrm{PG}(2,q^2)$ that contain $\mathcal{D}$.

Suppose that $\mathcal{B}$ is a blocking set of $\mathrm{PG}(2,q^h)$. Then $\mathcal{B}^* := \mathcal{B} \setminus \mathcal{D}$ blocks every line of type (i) in Π. Clearly, $\mathcal{B}^* \cup \mathcal{D}'$ is a blocking set of Π; however, $\mathcal{B}^*$ alone may not block all lines of type (ii) or ℓ'_∞. If $\mathcal{B} \cap \mathcal{D} = \varnothing$ and a line ℓ of type (ii) of Π is skew to $\mathcal{B}$, then ℓ is a blocking set of $\mathrm{PG}(2,q^h)$ disjoint from $\mathcal{B}$, thus $\mathcal{B} \cup \ell$ is a double blocking set in $\mathrm{PG}(2,q^h)$.

We choose a blocking set of $\mathrm{PG}(2,q^h)$ in the following way. Let $g(x) = x^q$. Similarly as before, the set of directions determined by $g(x)$ is $\{(1 : x^{q-1} : 0) \colon x \neq 0\} = \mathcal{D}$,

$$\mathcal{B}_0 := \underbrace{\{(y : 1 : y^q) : y \in \mathrm{GF}(q^h)\}}_{\mathcal{U}_0} \cup \underbrace{\{(1 : 0 : y^{q-1}) : y \in \mathrm{GF}(q^h)^*\}}_{\mathcal{D}_0}$$

is a blocking set of Rédei type in $\mathrm{PG}(2,q^h)$, and $\ell_\infty \cap \mathcal{B}_0 = \{(0 : 1 : 0)\} \notin \mathcal{D}$. Recall that $s_{-1}(x) = x^{-1}(x+1)^{q-1}$, and note that $0 \in V(s_{-1})$.

Definition 2.1. *For a point set $\mathcal{T} \subset \mathrm{PG}(2,q^h)$ and any element $a \in \mathrm{GF}(q^h)^*$, let $\sigma^{\mathcal{T}}_i(a) = |\{c \in \mathrm{GF}(q^h) \colon |\mathcal{U}(a,c) \cap \mathcal{T}| = i\}|$, and let the* type of a (with respect to $\mathcal{T}$) *be* $\sigma^{\mathcal{T}}(a) = (\sigma^{\mathcal{T}}_0(a), \sigma^{\mathcal{T}}_1(a), \ldots, \sigma^{\mathcal{T}}_{q^h}(a))$.

Lemma 2.2. *1. $\forall\, a \in \mathrm{GF}(q^h)^* \colon \mathcal{D}(a) \cap \mathcal{B}_0 = \varnothing$.*

2. $\forall\, a \in \mathrm{GF}(q^h)^* \colon \mathcal{U}(a,c) \cap \mathcal{D}_0 = \varnothing \iff c \notin D$.

3. If $a/a' \in C$, then $\sigma^{\mathcal{U}_0}(a) = \sigma^{\mathcal{U}_0}(a')$ and $\sigma^{\mathcal{B}_0}(a) = \sigma^{\mathcal{B}_0}(a')$.

4. $\forall\, a \in \mathrm{GF}(q^h)^*,\ c \in \mathrm{GF}(q^h) \colon \mathcal{U}(a,c) \cap \mathcal{U}_0 = \varnothing \iff$ $(c \neq 0$ and $-1/(c^{q-2}a^{q-1}) \notin V(s_{-1}))$ or $(c = 0$ and $a \notin C)$.

Proof. Let $a \in \mathrm{GF}(q^h)^*$, $c \in \mathrm{GF}(q^h)$, $f = f_{a,c}$ and $g(x) = x^q$. As $g(y) = 0 \iff y = 0$, $\mathcal{D}(a) \cap \mathcal{U}_0$ and $\mathcal{D}(a) \cap \mathcal{D}_0$ are clearly empty; thus $\mathcal{D}(a) \cap \mathcal{B}_0 = \varnothing$. Note that $f(x) = 0 \iff x^q = c$. Thus $\mathcal{U}(a,c) \cap \mathcal{D}_0$ is nonempty iff there exists $y \in \mathrm{GF}(q)^*$ such that $(y^{-(q-1)})^q = c$.

The left-hand-side is always a $(q-1)$-th power, so this is possible if and only if $c \in D$. In this case, $|\mathcal{U}(a,c) \cap \mathcal{D}_0| = 1$.

An element of $\mathcal{U}(a,c) \cap \mathcal{U}_0$ corresponds to elements $x, y \in GF(q^h)$ such that $(y : 1 : g(y)) = (x : f(x) : 1)$. Then $g(y) \neq 0$, so $y \neq 0$ and hence $x \neq 0$; clearly, $f(x) \neq 0$, 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 $g(x)f(x) = g(f(x)) = f(x)^q$, i.e., $x^q = (ax^q - ac)^{q-1} = a^{q-1}(x^q - c)^{q-1}$, equivalently:

$$\psi_c(x) := \frac{(x^q - c)^{q-1}}{x^q} = \frac{1}{a^{q-1}}. \qquad (\star)$$

Thus once $a \neq 0$ is fixed, $|\mathcal{U}(a,c) \cap \mathcal{U}_0|$ is the number of solutions of $(\star)$ in $\mathrm{GF}(q^h)$ in the indeterminate x.

Let $t \in \mathrm{GF}(q^h)^*$. Replacing x by $t^{(q-1)/q}x$ in $(\star)$, it is easy to see that $|\mathcal{U}(a,c) \cap \mathcal{U}_0| = |\mathcal{U}(t^{q-2}a, c/t^{q-1}) \cap \mathcal{U}_0|$. Moreover, as $c \in D \iff c/t^{q-1} \in D$, $|\mathcal{U}(a,c) \cap \mathcal{D}_0| = |\mathcal{U}(t^{q-2}a, c/t^{q-1}) \cap \mathcal{D}_0|$. Hence, if $a/a' \in C$, that is, $a' = a \cdot t^{q-2}$ for some $t \in \mathrm{GF}(q^h)^*$, then $\sigma^{\mathcal{U}_0}(a) = \sigma^{\mathcal{U}_0}(a')$ and $\sigma^{\mathcal{B}_0}(a) = \sigma^{\mathcal{B}_0}(a')$.

If $c = 0$, then $(\star)$ has a solution if and only if $a \in C$. Suppose now $c \neq 0$. Since $\{x^q \colon x \in \mathrm{GF}(q^h)^*\} = \{-cx \colon x \in \mathrm{GF}(q^h)^*\} = GF(q^h)^*$, the range of $\psi_c(x)$ is the same as that of $\frac{(-cx-c)^{q-1}}{-cx} = (-c)^{q-2}s_{-1}(x)$. Thus $\mathcal{U}(a,c) \cap \mathcal{U}_0 = \varnothing$ iff $-1/(c^{q-2}a^{q-1}) \notin V(s_{-1})$. □

Let C_a be the coset $(-1/a^{q-1})C$, and let $\chi_{\bar{C}}(a)$ be one or zero depending on whether $a \notin C$ or $a \in C$, respectively.

As $\gcd(q-2, q^h-1) = k$, $c \mapsto -1/(c^{q-2}a^{q-1})$ is a mapping from $\mathrm{GF}(q^h)^*$ to C_a which covers each element of the image exactly k times. Thus, by Lemma 2.2 (iv), for any $a \in D$ we have

$$\begin{gathered}\sigma_0^{\mathcal{U}_0}(a) = |\{c \in \mathrm{GF}(q^h) \colon \mathcal{U}(a,c) \cap \mathcal{U}_0 = \varnothing\}| = \\ |\{c \in \mathrm{GF}(q^h)^* \colon -1/(c^{p-2}a^{p-1}) \notin V(s_{-1})\}| + \chi_{\bar{C}}(a) = \\ |\mathrm{GF}(q^h)^*| - |V(s_{-1}) \cap C_a| \cdot k + \chi_{\bar{C}}(a).\end{gathered}$$

Recall that $0 \in V(s_{-1})$. Note that by Lemma 2.2 (3), $\sigma_0^{\mathcal{U}_0}$ is constant on any coset of C, hence, if the elements $a_1, \ldots, a_k \in D$ are representatives of the k cosets of C, then

$$|V(s_{-1})| = q^h - \sum_{i=1}^{k} \sigma_0^{\mathcal{U}_0}(a_i)/k + \sum_{i=1}^{k} \chi_{\bar{C}}(a)/k = q^h - \sum_{i=1}^{k} \sigma_0^{\mathcal{U}_0}(a_i)/k + \frac{k-1}{k}.$$

Note that each coset of C intersects D in $|D|/k$ points. Therefore we see that

$$\sum_{a \in D} \sigma_0^{\mathcal{U}_0}(a) = (|D|/k) \sum_{i=1}^{k} \sigma_0^{\mathcal{U}_0}(a_i),$$

thus $\sum_{a \in D} \sigma_0^{\mathcal{U}_0}(a)$ is divisible by $|D|/k$ and

$$|V(s_{-1})| = q^h - \frac{1}{|D|} \sum_{a \in D} \sigma_0^{\mathcal{U}_0}(a) + \frac{k-1}{k}. \qquad (1)$$

Thus the size of the value set $V(s_{-1})$ is determined by $\sum_{a \in D} \sigma_0^{\mathcal{U}_0}(a)$, which is of purely geometrical nature: it is the number of skew lines of type (ii) to $\mathcal{U}_0$ in the affine André plane $\Pi^A_{\mathcal{D}}$. In the case of $h = 2$, that is, Hall planes, lines of type (ii) are Baer subplanes of $\mathrm{PG}(2, q^2)$. Baer subplanes and their intersection properties are quite well understood in Desarguesian planes, which is well exploitable in the present context.

3 On Baer subplanes in $\mathrm{PG}(2, q^2)$

It is well-known that every subplane of a Desarguesian projective plane is itself a Desarguesian plane and hence, is coordinatised by the elements of a subfield of $\mathrm{GF}(q)$. In particular, we get that a Baer subplane of $\mathrm{PG}(2, q^2)$ corresponds to a set of $q^2 + q + 1$ points whose homogeneous coordinates, with respect to a well-chosen frame of $\mathrm{PG}(2, q^2)$, are in the subfield $\mathrm{GF}(q)$ of $\mathrm{GF}(q^2)$; a frame of a projective plane is a set of four points, no three of which are collinear. Likewise, a frame of $\mathrm{PG}(1, q^2)$ is a set of 3 distinct points and a *Baer subline* of $\mathrm{PG}(1, q^2)$ is defined as a set of $q+1$ points such that the coordinates with respect to a frame of $\mathrm{PG}(1, q^2)$, are in $\mathrm{GF}(q)$.

For a point $P \in \mathrm{PG}(2, q^2)$, let $\langle P \rangle$ denote the set of lines through P; that is, the pencil with carrier P. For two distinct points P and R, let $\langle P, R \rangle$ denote the line of $\mathrm{PG}(2, q^2)$ connecting P and R. Recall that given a Baer subplane $\mathcal{B}$ of $\mathrm{PG}(2, q^2)$, every line of $\mathrm{PG}(2, q^2)$ intersects $\mathcal{B}$ in one or $q + 1$ points. The lines of the latter type are called *long secants (of $\mathcal{B}$)*. Let $\langle P \rangle_{\mathcal{B}}$ denote the set of long secants of $\mathcal{B}$ through P. It is well-known that if $P \in \mathcal{B}$, then $|\langle P \rangle_{\mathcal{B}}| = q + 1$, and if $P \notin \mathcal{B}$, then $|\langle P \rangle_{\mathcal{B}}| = 1$.

Definition 3.1. *Let P be a point of $\mathrm{PG}(2, q^2)$ and let l be any line such that $P \notin l$. Choose a Baer subline m contained in l. Then the* Baer subpencil *determined by P and m is the set of $q + 1$ lines on P meeting l in a point of m.*

Note that if $\mathcal{B}$ is a Baer subplane and $P \in \mathcal{B}$, then $\langle P \rangle_{\mathcal{B}}$ is also a Baer subpencil of $\langle P \rangle$, as for any long secant line l of $\mathcal{B}$ not containing P, $\langle P \rangle_{\mathcal{B}}$ is determined by P and the Baer subline $l \cap \mathcal{B}$. Using the fact that the points of a frame in $\mathrm{PG}(2, q^2)$ or $\mathrm{PG}(1, q^2)$ determine a unique Baer subplane or subline respectively, we obtain the following well-known facts.

Lemma 3.2. *Given three collinear points in $\mathrm{PG}(2, q^2)$, there exists a unique Baer subline containing them. Dually, given three concurrent lines in $\mathrm{PG}(2, q^2)$, there exists a unique Baer subpencil containing them. Four points, no three of which are collinear, in $\mathrm{PG}(2, q^2)$, are contained in a unique Baer subplane.*

Let us remark that we could use not only $\mathcal{D}$ but any Baer subline of ℓ_∞ to construct the Hall plane. However, using $\mathcal{D}$ does not cause loss of generality, as the collineation group of $\mathrm{PG}(2, q^2)$ is transitive on the Baer sublines of a given line. We prove a couple of such transitivity results in connection with Baer subplanes and Baer sublines which might be known, yet seem to be hard to find a direct reference for. We use the well-known fact that the group $\mathrm{PGL}(3, q^2)$ of projective linear transformations of $\mathrm{PG}(2, q^2)$ is sharply transitive on the frames. For basic information on the collineations of $\mathrm{PG}(2, q^2)$

and $\mathrm{PG}(1,q^2)$ we refer to [11]. If a group G acts on a set Ω and $A_1,\dots,A_n$ are subsets of Ω, we denote by $\mathrm{Stab}_G(A_1,\dots,A_n)$ the subgroup of G that stabilises setwise each of the A_i's, $1 \leqslant i \leqslant n$. If $A_i = \{P\}$ is a single point, we write simply P instead of $\{P\}$.

Lemma 3.3. *Let $\mathcal{B}$ be an arbitrary Baer subplane of $\mathrm{PG}(2,q^2)$. For a point $Q \in \mathcal{B}$, $\mathcal{L}_Q$ denotes the set of tangent lines to $\mathcal{B}$ through Q. For a line ℓ tangent to $\mathcal{B}$, $\mathcal{X}_\ell$ denotes the set of all Baer sublines of ℓ, $\mathcal{X}'_\ell = \{\mathcal{R} \in \mathcal{X}_\ell \colon \mathcal{B} \cap \mathcal{R} = \varnothing\}$. For any line ℓ, $\mathcal{Y}_\ell$ denotes the set of all Baer subplanes that intersect ℓ in precisely one point, and for any fixed Baer subline $\mathcal{R}$ of ℓ, $\mathcal{Y}_{\ell,\mathcal{R}} = \{\mathcal{B}' \in \mathcal{Y}_l \colon \mathcal{B}' \cap \mathcal{R} = \varnothing\}$. Let us interpret $\mathrm{PGL}(3,q^2)$ and $\mathrm{PGL}(2,q^2)$ as the groups of all projective linear transformations of $\mathrm{PG}(2,q^2)$ and ℓ (after ℓ is fixed), respectively. Then the following hold.*

1. *Let $Q \in \mathcal{B}$. Then $\mathrm{Stab}_{\mathrm{PGL}(3,q^2)}(\mathcal{B},Q)$ is transitive on $\mathcal{L}_Q$.*
2. *Let ℓ' be any long secant to $\mathcal{B}$. Then $\mathrm{Stab}_{\mathrm{PGL}(3,q^2)}(\mathcal{B},\mathcal{B} \cap \ell')$ is transitive on $\ell' \setminus \mathcal{B}$.*
3. *Let ℓ be a tangent to $\mathcal{B}$ with tangency point Q. Then the actions of $\mathrm{Stab}_{\mathrm{PGL}(3,q^2)}(\mathcal{B},\ell)$ and $\mathrm{Stab}_{\mathrm{PGL}(2,q^2)}(Q)$ on ℓ are the same.*
4. *Let ℓ be a tangent to $\mathcal{B}$. Then $\mathrm{Stab}_{\mathrm{PGL}(3,q^2)}(\mathcal{B},\ell)$ is transitive on $\mathcal{X}'_\ell$.*
5. *Let $\mathcal{R}$ be a Baer subline of an arbitrary line ℓ. Then $\mathrm{Stab}_{\mathrm{PGL}(3,q^2)}(\mathcal{R})$ is transitive on $\mathcal{Y}_{\ell,\mathcal{R}}$.*

Proof. Let $Q \in \mathcal{B}$, and let ℓ be a line tangent to $\mathcal{B}$ on Q. Let ι be the mapping of $\mathrm{Stab}_{\mathrm{PGL}(3,q^2)}(\mathcal{B},\ell)$ into $\mathrm{Stab}_{\mathrm{PGL}(2,q^2)}(Q)$ given by the natural action of $\mathrm{Stab}_{\mathrm{PGL}(3,q^2)}(\mathcal{B},\ell)$ on ℓ. First we show that the kernel of this mapping is trivial. Suppose to the contrary that there exist a collineation $\varphi \in \mathrm{Stab}_{\mathrm{PGL}(3,q^2)}(\mathcal{B},\ell)$ that fixes ℓ pointwise, and that there exists a point $A \in \mathcal{B}$ such that $\varphi(A) \neq A$. Let e be a long secant of $\mathcal{B}$ through A such that $R := e \cap \ell$ is different from Q. Then $\langle R, A\rangle$ and $\varphi(\langle R, A\rangle) = \langle \varphi(R), \varphi(A)\rangle = \langle R, A'\rangle$ are two different long secants to $\mathcal{B}$ through R, a contradiction. Thus ι is an injection. As $\mathrm{PGL}(2,q^2)$ is sharply transitive on the triplets of ℓ, $|\mathrm{Stab}_{\mathrm{PGL}(2,q^2)}(Q)| = q^2(q^2-1)$, whence $|\mathrm{Stab}_{\mathrm{PGL}(3,q^2)}(\mathcal{B},\ell)| \leqslant q^2(q^2-1)$.

Let A, B and C be three points of $\mathcal{B}$ such that Q, A, B and C are in general position. As $\mathrm{Stab}_{\mathrm{PGL}(3,q^2)}(\mathcal{B},Q)$ is sharply transitive on such triplets, the image of A, B and C can be chosen in $(q^2+q)q^2(q^2-2q+1) = q^3(q+1)(q-1)^2$ ways, so this is the order of $\mathrm{Stab}_{\mathrm{PGL}(3,q^2)}(\mathcal{B},Q)$. Then $|\mathrm{Stab}_{\mathrm{PGL}(3,q^2)}(\mathcal{B},\ell)|$ is $|\mathrm{Stab}_{\mathrm{PGL}(3,q^2)}(\mathcal{B},Q)|$ divided by the size of the orbit of ℓ in $\mathcal{L}_Q$ under the action of $\mathrm{Stab}_{\mathrm{PGL}(3,q^2)}(\mathcal{B},Q)$, which is of size at most $|\mathcal{L}_Q| = q^2-q$. Hence $|\mathrm{Stab}_{\mathrm{PGL}(3,q^2)}(\mathcal{B},\ell)| \geqslant q^2(q^2-1)$. Consequently, equality holds, and thus $\mathrm{Stab}_{\mathrm{PGL}(3,q^2)}(\mathcal{B},Q)$ is transitive on $\mathcal{L}_Q$, and ι is a bijection, so $\mathrm{Stab}_{\mathrm{PGL}(3,q^2)}(\mathcal{B},\ell)$ acts on ℓ as $\mathrm{Stab}_{\mathrm{PGL}(2,q^2)}(Q)$ does. Thus (1) and (3) follow. (2) follows from (1) as $\mathrm{PG}(2,q^2)$ is self-dual.

As three points uniquely determine a Baer subline and $\mathrm{PGL}(2,q^2)$ is transitive on the triplets of ℓ, $\mathrm{PGL}(2,q^2)$ is transitive on $\mathcal{X}_\ell$. Let $\mathcal{R},\mathcal{R}' \in \mathcal{X}'_\ell$, and let $\varphi \in \mathrm{PGL}(2,q^2)$ be such that $\varphi(\mathcal{R}) = \mathcal{R}'$. By (2), we find $\psi \in \mathrm{Stab}_{\mathrm{PGL}(2,q^2)}(\mathcal{R})$ such that $(\psi \circ \varphi)(Q) = Q$. Thus $\psi \circ \varphi \in \mathrm{Stab}_{\mathrm{PGL}(2,q^2)}(Q)$ and it moves $\mathcal{R}$ to $\mathcal{R}'$; therefore $\mathrm{Stab}_{\mathrm{PGL}(2,q^2)}(Q)$ is transitive on $\mathcal{X}'_\ell$, and thus so is $\iota^{-1}(\mathrm{Stab}_{\mathrm{PGL}(2,q^2)}(Q)) = \mathrm{Stab}_{\mathrm{PGL}(3,q^2)}(\mathcal{B},\ell)$, which is assertion (4).

Now let ℓ be any line, let $\mathcal{R} \in \mathcal{X}_\ell$, and $\mathcal{B}_1, \mathcal{B}_2 \in \mathcal{Y}_\mathcal{R}$ arbitrary. As $\mathrm{PGL}(3,q^2)$ is transitive on the frames, there exists an element $\varphi_1 \in \mathrm{PGL}(3,q^2)$ such that $\varphi_1(\mathcal{B}_1) = \mathcal{B}_2$

and $\varphi_1(\mathcal{B}_1 \cap \ell) = \mathcal{B}_2 \cap \ell =: Q$. By (1), there exists $\varphi_2 \in \mathrm{Stab}_{\mathrm{PGL}(3,q^2)}(\mathcal{B}_2, Q)$ such that $\varphi_2 \circ \varphi_1(\ell) = \ell$. Then, by (4), there exists $\varphi_3 \in \mathrm{Stab}_{\mathrm{PGL}(3,q^2)}(\mathcal{B}, \ell)$ such that $\varphi_3 \circ \varphi_2 \circ \varphi_1(\mathcal{R}) = \mathcal{R}$. Thus (5) follows. □

By Lemma 3.3 (5), if $\mathcal{B}$ is a Baer subplane intersecting ℓ_∞ in a point Q and $\mathcal{R}$ is any Baer subline of ℓ_∞ not containing Q, we may assume without loss of generality that $\mathcal{B} = \mathcal{B}_0$ and $\mathcal{R} = \mathcal{D}$. We will need this only to prove one part of Lemma 3.10. Let us remark that if the collineation group of $\mathrm{PG}(2, q^2)$ were transitive on the ordered pairs of disjoint Baer subplanes, we would not need Lemma 3.3 to see this; however, this is not the case. For more details, see the work of Eisfeld [9].

Definition 3.4. *Let $[\mathcal{D}]$ be the set of Baer subplanes of $\mathrm{PG}(2, q^2)$ that contain $\mathcal{D}$. For a point $P \in \mathrm{AG}(2, q^2)$, let $[P] = [P]_{\mathcal{D}}$ denote the set of Baer subplanes that contain $\{P\} \cup \mathcal{D}$.*

In other words, $[P]$ is the set of lines of type (ii) through P, and $[\mathcal{D}]$ is the set of all lines of type (ii) in the Hall plane. The next result is well-known (basically this verifies the correctness of the construction of the Hall plane) yet we include a short proof.

Proposition 3.5. *Let $P, R \in \mathrm{AG}(2, q^2)$, $P \neq R$. If $\langle P, R\rangle \cap \ell_\infty \in \mathcal{D}$, then $|[P] \cap [R]| = 1$; otherwise $|[P] \cap [R]| = 0$. For any point $P \in \mathrm{AG}(2, q^2)$, $|[P]| = q + 1$.*

Proof. Let $P, R \in \mathrm{AG}(2, q^2)$, and let $Q_1, Q_2 \in \mathcal{D} \setminus \langle P, R\rangle$ arbitrary. By Lemma 3.2 there is a unique Baer subplane $\mathcal{B}$ containing P, R, Q_1, Q_2, so $|[P] \cap [R]| \leqslant 1$. The Baer subplane $\mathcal{B}$ has to contain the point $Q := \langle P, R\rangle \cap \ell_\infty$. If $Q \notin \mathcal{D}$, then clearly $\mathcal{B} \notin [\mathcal{D}]$ and $[P] \cap [R] = \varnothing$. If $Q \in \mathcal{D}$, then, since Q, Q_1 and Q_2 are distinct points, by Lemma 3.2, $\mathcal{D} \subset \mathcal{B}$, thus $\mathcal{B} \in [P] \cap [R]$.

Now let $P \in \mathrm{AG}(2, q^2)$ be arbitrary. Then the Baer subplanes in $[P]$ partition the $q^2 - 1$ points of each line $\langle P, Q\rangle \setminus \{P, Q\}$, $Q \in \mathcal{D}$ into subsets of size $q - 1$. We may conclude that $|[P]| = q + 1$. □

Definition 3.6. *Suppose that $P, R \in \mathrm{AG}(2, q^2)$. If $\langle P, R\rangle \cap \ell_\infty \in \mathcal{D}$, then let $[P, R]$ denote the unique Baer subplane containing $\{P, R\} \cup \mathcal{D}$ (cf. Proposition 3.5). We will say that $[P, R]$ exists if $\langle P, R\rangle \cap \ell_\infty \in \mathcal{D}$; otherwise we will say that $[P, R]$ does not exist.*

Definition 3.7. *Given a Baer subplane $\mathcal{B}$ of $\mathrm{PG}(2, q^2)$ such that $\mathcal{B} \cap \ell_\infty = \{Q\}$, $Q \notin \mathcal{D}$, let $\mathcal{S} = \mathcal{S}_{\mathcal{B}}$ be the set of lines of $\mathrm{PG}(2, q^2)$ meeting ℓ_∞ in a point of $\mathcal{D}$ and meeting $\mathcal{B}$ in $q + 1$ points.*

An *oval* of a projective plane of order q is a set of $q + 1$ points, no three of which are collinear. It is easy to see that every point of an oval $\mathcal{O}$ lies on a unique tangent line to $\mathcal{O}$; if q is odd, the tangent lines to an oval form a dual oval; and if q is even, all tangent lines to the oval $\mathcal{O}$ are concurrent. Moreover, there are $\frac{(q+1)q}{2}$ secant lines to $\mathcal{O}$ and $\frac{(q-1)q}{2}$ external lines to $\mathcal{O}$.

Lemma 3.8. *Let $\mathcal{B}$ be a Baer subplane of $\mathrm{PG}(2, q^2)$ such that $\mathcal{B} \cap \ell_\infty = \{Q\}$, $Q \notin \mathcal{D}$.*
(1) The set $\{\ell \cap \mathcal{B} \mid \ell \in \mathcal{S}\}$ is a dual oval of $\mathcal{B}$.

(2) A Baer subplane $\mathcal{B}' \in [\mathcal{D}]$ cannot contain three points of $\mathcal{B}$ that are collinear.

(3) For two distinct points $P, R \in \mathcal{B}$, $[P, R]_{\mathcal{D}}$ exists if and only if $\langle P, R\rangle \in \mathcal{S}$.

Proof. (1) As every point of $\mathcal{D} \subset \mathcal{B}$ lies on a unique $(q+1)$-secant to $\mathcal{B}$, $|\mathcal{S}| = |\mathcal{D}| = q+1$. Suppose that three lines of $\mathcal{S}$ meet in a point $P \in \mathcal{B}$. Then, by Lemma 3.2, the Baer subpencils $\mathcal{C} = \{\langle P, R\rangle \colon R \in \mathcal{D}\}$ and $\langle P\rangle_{\mathcal{B}}$ coincide. But as $Q \in \mathcal{B} \setminus \mathcal{D}$, $\langle P, Q\rangle \in \langle P\rangle_{\mathcal{B}} \setminus \mathcal{C}$, a contradiction. Hence, no three lines of $\mathcal{S}$ can meet in a common point, so the intersections of the lines of $\mathcal{S}$ with $\mathcal{B}$ form a dual oval of $\mathcal{B}$.

(2) Assume that a Baer subplane $\mathcal{B}' \in [\mathcal{D}]$ contains three points of $\mathcal{B}$ that are collinear. These three points determine a line of $\mathrm{PG}(2, q^2)$ meeting $\mathcal{B}$ and $\mathcal{B}'$ in the same Baer subline l, which necessarily meets the Baer subline $\mathcal{D} \subset \mathcal{B}'$, a contradiction since $\mathcal{B} \cap \mathcal{D} = \varnothing$.

(3) As $\langle P, R\rangle$ is a long secant of $\mathcal{B}$, this follows immediately from the definition of $\mathcal{S}$ and Proposition 3.5. □

Lemma 3.9. *Let $\mathcal{B}$ be a Baer subplane of $\mathrm{PG}(2, q^2)$ such that $\mathcal{B} \cap \ell_\infty = \{Q\}$, $Q \notin \mathcal{D}$. Call $\mathcal{O}$ the set of tangent points of $\mathcal{S}$ in $\mathcal{B}$, i.e. the set of points of $\mathcal{B}$ that are contained in exactly one line of $\mathcal{S}$. Call $\mathcal{O}^+$ the set of points of $\mathcal{B}$ covered by exactly two lines of $\mathcal{S}$ and call $\mathcal{O}^-$ the set of points of $\mathcal{B} \setminus \{Q\}$ not covered by any line of $\mathcal{S}$.*

(1) $|\mathcal{O}| = q+1$, $|\mathcal{O}^+| = \frac{q(q+1)}{2}$, $|\mathcal{O}^-| = \frac{(q+1)(q-2)}{2}$. If q is odd, then $\mathcal{O}$ is an oval of $\mathcal{B}$; if q is even, then $\mathcal{O}$ is a line of $\mathcal{B}$.

(2) If $P \in \mathcal{O}^-$, then each Baer subplane of $[P]$ meets $\mathcal{B}$ only in P.

(3) If $P \in \mathcal{O}$, then q Baer subplanes of $[P]$ meet $\mathcal{B}$ in two points, one of which is P and the other is contained in $\mathcal{O}^+$, and one Baer subplane of $[P]$ meets $\mathcal{B}$ only in P.

(4) If $P \in \mathcal{O}^+$, then $q-1$ Baer subplanes of $[P]$ meet $\mathcal{B}$ in three points of $\mathcal{O}^+$ (including P), and two Baer subplanes of $[P]$ meet $\mathcal{B}$ in two points, one of which is P and the other is contained in $\mathcal{O}$.

Proof. (1) By Lemma 3.8, the set $\mathcal{O}^* = \{l \cap \mathcal{B} | l \in \mathcal{S}\}$ is a dual oval of $\mathcal{B}$. Note that Q in not covered by $\mathcal{O}^*$. Applying dually the aforementioned properties of ovals to $\mathcal{O}^*$ (so $\mathcal{O}$, $\mathcal{O}^+$ and $\mathcal{O}^-$ correspond dually to the tangents, the secant lines and external lines of an oval, resp.), the assertion follows.

(2) As $P \in \mathcal{O}^-$, this follows immediately from Lemma 3.8 (3).

(3) Let $P \in \mathcal{O}$. Consider the unique line $l \in \mathcal{S}$ on P. By Lemma 3.8 (3), for a point $P' \in \mathcal{B} \setminus \{P\}$, $[P, P'] \in [P]$ exists if and only if $P' \in l \setminus \{P\}$. Since a Baer subplane $\mathcal{B}' \in [P]$ cannot contain three points of $\mathcal{B}$ that are collinear by Lemma 3.8 (2), $|\{[P, P'] \colon P' \in l \setminus \{P\}\}| = q$. By Proposition 3.5, there is one Baer subplane left in $[P]$. If this subplane contained a point Q of $\mathcal{B} \setminus \{P\}$, then $\langle P, Q\rangle$ would be a line of $\mathcal{S}$ by Lemma 3.8 (3), a contradiction since this would force P to be contained in $\mathcal{O}^+$.

(4) Let $P \in \mathcal{O}^+$, and denote by ℓ_1, ℓ_2 the two lines of $\mathcal{S}$ on P. By Lemma 3.8 and Proposition 3.5 we see that each of the $2q$ points of $(\ell_1 \cup \ell_2) \cap (\mathcal{B} \setminus \{P\})$ is covered by exactly one of the $q+1$ Baer subplanes of $[P]$. Since $\mathcal{O}^*$ is a dual oval in $\mathcal{B}$, for $i = 1, 2$, there is exactly one point of ℓ_i in $\mathcal{B}$, say R_i, that only lies on the line ℓ_i of $\mathcal{S}$, hence, $R_i \in \mathcal{O}$. Then, by (3), $[P, R_i] \cap \mathcal{B} = \{P, R_i\}$, $i = 1, 2$. It follows that the $q-1$

Baer subplanes of $[P] \setminus \{[P, R_1], [P, R_2]\}$ each contain a point of $\ell_1 \setminus \{P\}$ and a point of $\ell_2 \setminus \{P\}$. □

Lemma 3.10. *Let $\mathcal{B}$ be a Baer subplane of* $\mathrm{PG}(2, q^2)$ *such that* $\mathcal{B} \cap \ell_\infty = \{Q\}$*,* $Q \notin \mathcal{D}$*. Let* $P \in \mathcal{D}'$ *be a point of the Hall plane* $\Pi_{\mathcal{D}}$*, and let* $t_i(P)$ *denote the number of* i*-secant lines (of type (ii)) through* P *to* $\mathcal{B}^* := \mathcal{B} \setminus \{Q\}$*. If* $q \not\equiv 2 \pmod 3$*, then* $\forall\, P \in \mathcal{D}'\colon t_0(P) = (q^2 - q)/3$*. If* $q \equiv 2 \pmod 3$*, then for* $(q+1)/3$ *points* $P \in \mathcal{D}'\colon t_0(P) = (q^2 - q - 2)/3$*, and for* $2(q+1)/3$ *points* $P \in \mathcal{D}'\colon t_0(P) = (q^2 - q + 1)/3$*.*

Proof. Let P be a point of $\mathcal{D}'$ and note that lines of $\mathcal{H}$ through the point P of $\mathcal{D}'$ are necessarily lines of type (ii). By Lemma 3.9, a line tangent to $\mathcal{B}^*$ contains either a point of $\mathcal{O}^-$ or $\mathcal{O}$, denote the number of such tangents by $t_1'(P)$ and $t_1''(P)$, respectively; a 2-secant to $\mathcal{B}^*$ contains one point of $\mathcal{O}$ and one of $\mathcal{O}^+$; a 3-secant to $\mathcal{B}^*$ contains three points of $\mathcal{O}^+$. Thus we have $t_1'(P) = |\mathcal{O}^-| = (q+1)(q-2)/2$, $t_1''(P) + t_2(P) = |\mathcal{O}| = q+1$ and $t_2(P) + 3t_3(P) = |\mathcal{O}^+| = q(q+1)/2$. From these equations, we get that the total number of lines of type (ii) intersecting $\mathcal{B}^*$ through P is $t_1'(P) + t_1''(P) + t_2(P) + t_3(P) = 2q(q+1)/3 - t_2(P)/3$. It follows that if $q \not\equiv 2 \pmod 3$, then $t_2(P) \equiv q \pmod 3$, and if $q \equiv 2 \pmod 3$, then $t_2(P) \equiv 0 \pmod 3$.

By Lemma 3.9, each of the $q+1$ points in $\mathcal{O}$ determines q 2-secants to $\mathcal{B}$ through some points of $\mathcal{D}'$. Moreover, all these 2-secants are different and every 2-secant line of type (ii) is obtained in this way, so we get $\sum_{P \in \mathcal{D}'} t_2(P) = (q+1)q$. Thus, since $|\mathcal{D}'| = q+1$, and $|t_2(P)| \leqslant |\mathcal{O}| = q+1$, either there exists a point $P \in \mathcal{D}'$ such that $t_2(P) = q+1 \not\equiv q \pmod 3$ and hence $q \equiv 2 \pmod 3$, or for all points $P \in \mathcal{D}'\colon t_2(P) = q$.

Suppose now $q \equiv 2 \pmod 3$ (that is, $k = 3$). By Lemma 3.3 (5), we may assume without loss of generality that $\mathcal{B} = \mathcal{B}_0$. If $P = (a)$ then $t_i(P) = \sigma_i^{\mathcal{B}_0}(a)$, hence by Lemma 2.2 (3) we have that $\mathcal{D}'$ can be partitioned into three sets of size $(q+1)/3$, and on each of these sets, $t_2(P)$ takes on the same value. As $3 \mid t_2(P)$ and there must be some $P \in \mathcal{D}'$ with $t_2(P) < q+1$, it is easy to see that $t_2(P) = q-2$ on one of these sets, and $t_2(P) = q+1$ on the two remaining sets.

By considering $t_0(P) = q^2 - \frac{2q(q+1)}{3} + \frac{t_2(P)}{3}$, we can finish the proof easily. □

4 Some blocking and double blocking sets

First, starting from the Hall plane, we give the construction of interesting small blocking sets in non-Desarguesian planes.

Theorem 4.1. *In the projective Hall plane* Π *of order* q^2*,* $q \geqslant 3$*, there exists a minimal blocking set of size* $q^2 + 2q + 2$*, which admits* 1-, 2-, 3-, 4-, $(q+1)$- *and* $(q+2)$*-secants.*

Proof. Let $\mathcal{D}$ be a Baer subline of ℓ_∞ in $\mathrm{PG}(2, q^2)$ and let, as before, $\mathcal{D}'$ denote the set of derived directions. Let $\mathcal{B}$ be a Baer subplane of $\mathrm{PG}(2, q^2)$ such that $\mathcal{B} \cap \ell_\infty$ is a single point $Q \notin \mathcal{D}$. Then it is clear that $\mathcal{T} := \mathcal{B} \cup \mathcal{D}'$ is a blocking set of $\mathcal{H}$ of size $q^2 + 2q + 2$. We claim that $\mathcal{T}$ is a minimal blocking set. By Lemma 3.10, the points of $\mathcal{D}'$ are essential for $\mathcal{T}$. The points of $\mathcal{B}$ (including Q) are also essential, as there are at least

$q^2+1-|\langle P\rangle_{\mathcal{B}}|-|\mathcal{D}'|=q^2-2q-1>0$ tangents on each point P of $\mathcal{B}$. This proves our claim. Using Lemma 3.9, we see that a line of type (ii) meets $\mathcal{T}$ in either 2, 3 or 4 points. A line of type (i) meets $\mathcal{T}$ in 1 or $q+1$ points and ℓ_∞ meets $\mathcal{T}$ in $q+2$ points. □

Remark 4.2. *Using similar ideas, we could also show that in the projective Hall plane of order q^2, $q \geqslant 3$, there also exists a minimal blocking set of size q^2+2q+1 or q^2+2q.*

Theorem 4.3. *Let q be a prime power. There exists a non-Desarguesian affine plane of order q^2 in which there is a blocking set of size at most $4q^2/3+5q/3$.*

Proof. Consider the blocking set $\mathcal{T}$ of size q^2+2q+2 in the Hall plane $\mathcal{H}$, constructed in Theorem 4.1. By Lemma 3.10, we may choose a point $P \in \mathcal{D}'$ that has at most $(q^2-q-2)/3$ or exactly $(q^2-q)/3$ tangents to $\mathcal{T}$ through it, according to whether $q \equiv 2 \pmod 3$ or not, respectively. Let ℓ be one of these tangents. By putting one point on all skew lines of $\mathcal{T}\setminus\{P\}$ but ℓ, we obtain an affine blocking set in $\mathcal{H}\setminus\ell$ of size at most $4q^2/3+5q/3$. □

Note that the ratio of the size of the above constructed affine blocking set and the order of the plane tends to 4/3, which is notably smaller than the ratio 2 in case of Desarguesian affine planes.

Remark 4.4. *We may also use multiple derivation to achieve similar results. That is, let $\mathcal{D}_1,\dots,\mathcal{D}_n$ be pairwise disjoint Baer sublines of ℓ_∞ in $\mathrm{PG}(2,q^2)$, $q \geqslant 3$, $1 \leqslant n < q-2$, replace the lines intersecing ℓ_∞ in $\mathcal{D}_1\cup\dots\cup\mathcal{D}_n$ by the Baer subplanes $[\mathcal{D}_1]\cup\dots\cup[\mathcal{D}_n]$, and consider the resulting projective plane Π. Take a Baer subplane $\mathcal{B}$ of $\mathrm{PG}(2,q^2)$ such that $\mathcal{B}\cap\ell_\infty=\{Q\}$, $Q\notin\mathcal{D}_1\cup\dots\cup\mathcal{D}_n$. Then Lemma 3.10 shows that $\mathcal{T}=\mathcal{B}\cup\mathcal{D}_1\cup\dots\cup\mathcal{D}_n$ is a blocking set in Π for which all points of $\mathcal{T}\cap\ell_\infty$ are essential; moreover, as on each point of $\mathcal{B}\setminus\{Q\}$ there are at least $q^2+1-(n+1)(q+1)>0$ tangents to $\mathcal{T}$, $\mathcal{T}$ is minimal. Thus in the resulting projective plane we obtain a minimal blocking set of size $q^2+(n+1)(q+1)$; and, as in Theorem 4.3, we find an affine plane of order q^2 with a blocking set of size at most $4q^2/3+(3n+2)q/3+n-1$.*

Next we discuss blocking sets of the André planes $\Pi_{\mathcal{D}}$ and double blocking sets of $\mathrm{PG}(2,q^h)$. In the proof of the next theorem, we will use the following result.

Result 4.5 (Bacsó–Héger–Szőnyi [1]). *Let $\mathcal{F}$ be a finite field of characteristic p, and let $H \leqslant \mathcal{F}^*$ be a multiplicative subgroup of m elements. Suppose that $g\in\mathcal{F}[x]$ maps a coset c_1H into another coset c_2H. Then the mapping $g|_{c_1H}\colon c_1H\to c_2H$ is injective if and only if the constant term of $g(c_1x)^t \pmod{x^m-1}$ is zero for all $1\leqslant t\leqslant m-1$, $p\nmid t$.*

Theorem 4.6. *Suppose that $k=\gcd(q-2,q^h-1)=1$, $h\geqslant 2$. Then for each $a\in D$, there exists $c\in\mathrm{GF}(q^h)^*$ such that $\mathcal{B}(a,c)$ and $\mathcal{B}_0$ are disjoint.*

Proof. Recall that $s_{-1}(x)=(x+1)^{q-1}/x$. By Lemma 2.2, we have to find $c\in\mathrm{GF}(q^h)^*$, $c\notin D$ such that $-1/(c^{q-2}a^{q-1})\notin V(s_{-1})$. Clearly, $c\in D$ iff $-1/(c^{q-2}a^{q-1})\in -D$; thus if we find an element $0\neq t\notin -D$, $t\notin V(s_{-1})$, then, by $\gcd(q-2,q^h-1)=1$, the unique element $c \in \mathrm{GF}(q^h)^* \setminus D$ defined by $c^{q-2} = -1/(ta^{q-1})$ is appropriate. Note that for any $r \in \mathrm{GF}(q^h)^*$, $s_{-1}(x) \in rD$ iff $x \in r^{-1}D$. Choose r so that $r^{-1}D \neq -D$. Then it is enough to show that $s_{-1}|_{rD} \colon rD \to r^{-1}D$ is not a bijection.

By Result 4.5, it is enough to show that the constant term of $\psi(rx) \pmod{x^m - 1}$ is nonzero, where $\psi(x) = x^{q^h-2}(x+1)^{q-1}$ and $m = |D| = (q^h - 1)/(q-1)$. Now

$$\psi(rx) = (rx+1)^{q-1}(rx)^{q^h-2} = \sum_{i=0}^{q-1} \binom{q-1}{i} (rx)^{i+q^h-2},$$

and precisely those addends contribute to the constant term of $\psi(rx) \pmod{x^m - 1}$ whose exponents are divisible by m. As $m \mid q^h - 1$ and $q - 1 < (q^h - 1)/(q-1) = m$, we see that $i + q^h - 2 \equiv i - 1 \equiv 0 \pmod{m}$ if and only if $i = 1$ (under $0 \leqslant i \leqslant q-1$). As $\binom{q-1}{1} r^{q^h-1} = -1$ is clearly nonzero, the proof is finished. □

Corollary 4.7. *Let* $\gcd(q-2, q^h-1) = 1$, $h \geqslant 2$, $q \geqslant 4$ *a power of the prime* p. *Then, in the André plane* $\Pi_{\mathcal{D}}$ *of order* q^h, *there exists a minimal blocking set of size* $q^h + 2(q^h-1)/(q-1)$ *admitting a* t*-secant, with* $t = (q^h-1)/(q-1) + 1 \not\equiv 1 \pmod{p}$.

Proof. It is clear that $\mathcal{B} := \mathcal{B}_0 \cup \mathcal{D}'$ is a blocking set in Π of size $q^h + 2(q^h-1)/(q-1)$. By Theorem 4.6, all points of $\mathcal{D}'$ are essential. On the other hand, by Result 1.4, in $\mathrm{PG}(2, q^h)$ there are at least $q^h - 2(q^h-1)/(q-1) + 1$ tangents to $\mathcal{B}_0$ in each point of $\mathcal{B}_0$. As at least $q^h - 3(q^h-1)/(q-1) + 1 > 0$ of these tangents are also lines of Π, the points of $\mathcal{B}_0$ are also all essential. The line ℓ'_∞ is a $(q^h-1)/(q-1)+1$-secant of Π. □

Just as in case of starting with a Hall plane, one may use the same ideas to construct small blocking sets in non-Desarguesian affine planes coming from the André plane $\Pi_{\mathcal{D}}$. If for a point $P \in \mathcal{D}'$ there are t_1 tangents to $\mathcal{B}_0 \cup \mathcal{D}'$, we may obtain an affine plane of order q^h admitting a blocking set of size $q^h + 2(q^h-1)/(q-1) + t_1 - 2 \approx (1 + 2/(q-1) + t_1/q^h)q^h$. Using the GAP package FinInG [10, 2], we have computed the number of tangents on points of $\mathcal{D}'$ for several values of q and h. The results are shown in Table 1.

As a consequence of Theorem 4.6, we see that there exist two disjoint blocking sets of size $q^h + (q^h-1)/(q-1)$ in $\mathrm{PG}(2, q^h)$ (namely, $\mathcal{B}_0$ and $\mathcal{B}(a, c)$ with properly chosen parameters); thus their union is a small double blocking set. Such a double blocking set was already obtained in [1] in which the following theorem is shown.

Result 4.8 (Bacsó–Héger–Szőnyi [1]). *Let* $\tau_2(\mathrm{PG}(2,s))$ *denote the size of the smallest minimal double blocking set of* $\mathrm{PG}(2,s)$, *then* $\tau_2(\mathrm{PG}(2,s)) \leqslant 2\left(s + \frac{s-1}{r-1}\right)$, *where* r *is the size of the largest proper subfield of* $\mathrm{GF}(s)$.

In the same paper, the authors use this bound on τ_2, the size of the smalles double blocking set, to determine the so-called *upper chromatic number* of the projective plane of order q, which is easily seen to be at least $q^2 + q + 2 - \tau_2$.

Next we describe other small double blocking sets obtained as the union of two disjoint blocking sets. As a corollary, we will construct a minimal blocking set in the André plane $\Pi_{\mathcal{D}}$ of order q^h, strictly containing a blocking set of the corresponding Desarguesian

q	h	q^h	t_1	$\lvert\mathcal{B}^A\rvert$	t_1/q^h	$\lvert\mathcal{B}^A\rvert/q^h$
3	3	27	6	57	0.222	2.111
3	4	81	20	197	0.247	2.21
3	5	243	60	543	0.247	2.235
4	3	64	12	116	0.188	1.813
4	4	256	60	484	0.234	1.891
4	5	1024	220	1924	0.215	1.879
5	3	125	36	221	0.288	1.768
5	4	625	162	1097	0.259	1.755
5	5	3125	875	5560	0.28	1.779
7	3	343	108	563	0.315	1.641
7	4	2401	731	3930	0.304	1.637
7	5	16807	5175	27582	0.308	1.641
8	3	512	126	782	0.246	1.527
8	4	4096	918	6182	0.224	1.509
8	5	32768	8070	50198	0.246	1.532
9	3	729	231	1140	0.317	1.564
9	4	6561	2148	10347	0.327	1.577
9	5	59049	19090	92899	0.323	1.573
11	3	1331	447	2042	0.336	1.534
11	4	14641	4716	22283	0.322	1.522
13	3	2197	759	3320	0.345	1.511
13	4	28561	9676	42995	0.339	1.505
16	3	4096	1079	5719	0.263	1.396
16	4	65536	17696	91968	0.27	1.403
17	3	4913	1701	7226	0.346	1.471
19	3	6859	2394	10013	0.349	1.46
23	3	12167	4158	17429	0.342	1.432
25	3	15625	5589	22514	0.358	1.441
27	3	19683	7002	28197	0.356	1.433
29	3	24389	8715	34844	0.357	1.429
32	3	32768	9060	43940	0.276	1.341
37	3	50653	17935	71400	0.354	1.41

Table 1: $\mathcal{B}_0 \cup \mathcal{D}'$ is a blocking set in the André plane $\Pi_{\mathcal{D}}$ of order q^h, t_1 is the minimum of the number of tangents to $\mathcal{B}_0 \cup \mathcal{D}'$ through P, where P ranges through $\mathcal{D}'$, $\mathcal{B}^A$ is the affine blocking set constructed from $\mathcal{B}_0 \cup \mathcal{D}'$ in the mentioned way. Note that t_1 is particularly small if q is even and, for fixed h, $|\mathcal{B}^A|/q^h$ is decreasing in q if q is prime. Let us remark that for $q = 32$, $h = 3$, $|\mathcal{B}^A|$ is smaller than $\left\lfloor \frac{4}{3}q^h + \frac{5}{3}\sqrt{q^h} \right\rfloor$ by 52.

projective plane, but which is smaller than the one obtained in Corollary 4.7 if q is a prime. Moreover, if $q = p^h$, where p and h are prime, we find a smaller upper bound for $\tau_2(\mathrm{PG}(2, p^h))$ than the one of Result 4.8, which also improves in that case the results on the upper chromatic number. For this construction, we will need the notion of *linear blocking sets*.

By *field reduction*, the points of $\mathrm{PG}(2, q^h)$ are in one-to-one correspondence with the elements of a Desarguesian $(h-1)$-spread $\mathcal{S}$ in $\mathrm{PG}(3h-1, q)$ (as both kinds of objects can be interpreted as h-dimensional subspaces of a $3h$ dimensional vectorspace over $\mathrm{GF}(q)$). Let $\mathcal{B}(\mu)$ denote the set of spread elements of $\mathcal{S}$ meeting a subspace μ of $\mathrm{PG}(3h-1, q)$. We often identify the element of $\mathcal{S}$ with the corresponding point in $\mathrm{PG}(2, q^h)$. The spread element corresponding to a point P of $\mathrm{PG}(2, q^h)$ will be denoted as $\bar{P}$. If π is an h-space of $\mathrm{PG}(3h-1, q)$, then it is clear that $\mathcal{B}(\pi)$ is a blocking set in $\mathrm{PG}(2, q^h)$, and such a blocking set is an $\mathrm{GF}(q)$-*linear blocking set*. Note that a linear blocking set is necessarily minimal and its size is at most $(q^{h+1}-1)/(q-1)$. For more information on field reduction and linear sets, we refer to [14].

We say that $\mathcal{B}(\pi)$ is of *vertex-type* if it is non-trivial and there exists one spread element of $\mathcal{S}$, say V, which meets the h-space π in an $(h-2)$-space. It is easy to see that a blocking set of vertex-type consists of $q+1$ $(q^{h-1}+1)$-secants through the point V and thus has size $q^h + q^{h-1} + 1$. It follows from [15] that $\mathcal{B}(\pi)$ is projectively equivalent to the set of points $\{(\mathrm{Tr}(x) : 1 : x) | x \in \mathrm{GF}(q^h)\} \cup \{(\mathrm{Tr}(x) : 0 : x) \mid x \in \mathrm{GF}(q^h)^*\}$, where Tr denotes the trace function from $\mathrm{GF}(q^h)$ to $\mathrm{GF}(q)$, i.e. $\mathrm{Tr} : \mathrm{GF}(q^h) \to \mathrm{GF}(q)$, $x \mapsto x + x^q + x^{q^2} + \ldots + x^{q^{h-1}}$.

Theorem 4.9. *Let $p > 5$ and let $\mathcal{B}$ be a non-trivial blocking set in $\mathrm{PG}(2, p^h)$, p prime, of size $|\mathcal{B}| \leqslant \frac{3}{2}(p^h - p^{h-1})$ (e.g., a non-trivial linear blocking set with $p > 5$), then there exists a blocking set of vertex-type $\mathcal{B}(\pi)$ such that $\mathcal{B} \cap \mathcal{B}(\pi) = \varnothing$.*

Proof. Let Q be a point of $\mathrm{PG}(2, p^h)$, not contained in $\mathcal{B}$. Using that every line through Q meets $\mathcal{B}$ in 1 mod p points by Result 1.1, this implies that there are at least $p^h + 1 - (|\mathcal{B}| - p^h - 1)/p$ tangent lines through Q to $\mathcal{B}$. It is clear that the intersection points of the tangent lines with $\mathcal{B}$ cannot be collinear, since otherwise either $\mathcal{B}$ would be a trivial blocking set, or the size of $\mathcal{B}$ would be at least $2p^h + 1 - (|\mathcal{B}| - p^h - 1)/p > \frac{3}{2}(p^h - p^{h-1})$. Now consider 3 non-collinear points P_1, P_2, P_3 such that QP_i is a tangent line to $\mathcal{B}$.

Choose a point T of $\bar{Q}$ (i.e. the spread element corresponding to Q), and consider the $2h$-space τ through $\bar{P}_1$, $\bar{P}_2$, and the point T, then τ meets $\bar{Q}$ only in the point T. Denote the point set of the spread elements of $\mathcal{B}$ by $\tilde{B}$. Let μ be an $(h-2)$-space in $\bar{Q}$, not through T. We may consider τ to be the quotient space $\mathrm{PG}(3h-1, p)/\mu$; every point R of $\mathrm{PG}(3h-1, p)$, not in μ corresponds to the projection of R from μ onto the space τ.

We claim that there exists a line ℓ in $\mathrm{PG}(3h-1, p)/\mu$, skew from $\tilde{B}/\mu$. Suppose to the contrary that $\tilde{B}/\mu$ is a blocking set with respect to lines in $\mathrm{PG}(3h-1, p)/\mu \cong \mathrm{PG}(2h, p)$. The set $\tilde{B}/\mu$ contains at most $\left(\frac{p^h-1}{p-1}\right)\frac{3}{2}\left(p^h - p^{h-1}\right)$ points, which is less than $3(p^{2h-1}+1)/2$. Hence, $\tilde{B}/\mu$ is a small blocking set with respect to lines in $\mathrm{PG}(2h, p)$, and so by [21], all essential points are contained in a hyperplane. Let R_i, $i = 1, 2$ be some point contained in $\bar{P}_i$ and let R_3 be the point $\bar{P}_3 \cap \tau$.

Suppose that line $\langle T, R_i\rangle$ contains a point $X \neq R_i$ of $\tilde{B}/\mu$. Then $\langle \mu, X\rangle$ would contain a point Y of $\tilde{B}$, such that $\mathcal{B}(Y)$ is a point of $\mathcal{B}$, different from P_i. Now $\mathcal{B}(Y)$ lies on the tangent line $\langle Q, P_i\rangle$ since $\langle \mu, X\rangle$ lies in $\langle \bar{Q}, \bar{P_i}\rangle$. It follows from the fact that $X \neq R_i$ that $\mathcal{B}(Y)$ is different from P_i. Hence, $\langle T, R_i\rangle$ only contains the point R_i of $\tilde{B}/\mu$ which implies that the points of $\bar{P}_1$, $\bar{P}_2$ are essential points and we recall that all essential points are contained in a hyperplane, which is then necessarily $\langle \bar{P}_1, \bar{P}_2\rangle$. But since P_1, P_2, P_3 are not collinear, the point R_3, which is clearly essential, is not contained in $\langle \bar{P}_1, \bar{P}_2\rangle$, a contradiction. This proves our claim.

So we find a line ℓ in τ, skew from $\tilde{B}/\mu$. The space $\pi = \langle \ell, \mu\rangle$ is an h-space such that $\mathcal{B}(\pi) \cap \mathcal{B} = \varnothing$. Since π meets $\bar{Q}$ in the $(h-2)$-space μ, $\mathcal{B}(\pi)$ is a blocking set of vertex-type meeting the required conditions. □

Corollary 4.10. *If $\mathcal{B}$ is a blocking set in* $\mathrm{PG}(2, p^h)$*, $p > 5$ prime, of size at most $\frac{3}{2}(p^h - p^{h-1})$, then there exists a double blocking set in* $\mathrm{PG}(2, p^h)$ *of size $|\mathcal{B}| + p^h + p^{h-1} + 1$. In particular, if $p > 5$, then there exist double blocking sets in* $\mathrm{PG}(2, p^h)$ *of size $2p^h + 2p^{h-1} + 2$ and $\tau_2(\mathrm{PG}(2, p^h)) \leqslant 2\left(p^h + p^{h-1} + 1\right)$.*

Corollary 4.11. *Consider the André plane $\Pi_{\mathcal{D}}$ of order p^h derived from* $\mathrm{PG}(2, p^h)$*, p prime, $h \geqslant 2$. Then there exists a non-trivial minimal blocking set in $\Pi_{\mathcal{D}}$ of size at least $p^h + p^{h-1} + 2$ and at most $p^h + p^{h-1} + \frac{p^h-1}{p-1} + 1$.*

Proof. Consider the blocking set $\mathcal{B}_1 = \mathcal{B}(1, 0)$ of $\mathrm{PG}(2, p^h)$ as defined earlier. From Theorem 4.9, we obtain that there is a blocking set $\mathcal{B}_2$ of size $p^h + p^{h-1} + 1$ skew from $\mathcal{B}_1$. Clearly, $\mathcal{T} := \mathcal{B}_2 \cup \mathcal{D}'$ forms a blocking set of size $p^h + p^{h-1} + \frac{p^h-1}{p-1} + 1$ in Π. Since $\mathcal{B}_1$ (considered as a line of Π) and $\mathcal{T}$ are skew, at least one point of $\mathcal{D}'$ is essential to the blocking set $\mathcal{T}$. Moreover, it is clear that every point of $\mathcal{B}_2$ is essential to $\mathcal{T}$ and the statement follows. □

As an addition, using the same method, we construct small double blocking sets with respect to k-spaces in $\mathrm{PG}(2k, p^h)$. Note that a $\mathrm{GF}(p)$-linear blocking set with respect to k-spaces in $\mathrm{PG}(2k, p^h)$, p prime, is a set $\mathcal{B}(\pi)$, where π is an hk-dimensional subspace of $\mathrm{PG}(h(2k+1)-1, p)$ and that such a linear blocking set is necessarily minimal.

Theorem 4.12. *Let $p > 5$. There exist two sets $\mathcal{B}(\pi)$ and $\mathcal{B}(\pi')$, where π and π' are hk-dimensional subspaces of* $\mathrm{PG}(h(2k+1)-1, p)$ *with $\mathcal{B}(\pi) \cap \mathcal{B}(\pi') = \varnothing$.*

Proof. Let π be an hk-dimensional space in $\mathrm{PG}(h(2k+1)-1, p)$ and denote the point set of the spread elements in $\mathcal{B}(\pi)$ by $\tilde{S}$, then $|\tilde{S}| = |\mathcal{B}(\pi)| \cdot \frac{p^h-1}{p-1} \leqslant \frac{p^{hk+1}-1}{p-1} \cdot \frac{p^h-1}{p-1}$. If $p > 5$, then $\frac{p^{hk+1}-1}{p-1} \cdot \frac{p^h-1}{p-1} < \frac{3}{2}(p^{hk+h-1} + 1)$. This implies that, if $\tilde{S}$ blocks all hk-spaces, it is a small blocking set with respect to hk-spaces in $\mathrm{PG}(h(2k+1)-1, p)$, and hence, $\tilde{S}$ is an $(hk+h-1)$-dimensional subspace of $\mathrm{PG}(h(2k+1)-1, p)$. This implies that $\mathcal{B}(\pi)$ is the set of all spread elements contained in an $(h(k+1)-1)$-dimensional subspace spanned by spread elements, hence, $\mathcal{B}(\pi)$ corresponds to a k-space of $\mathrm{PG}(2k, p^h)$. This implies that if π is an hk-dimensional subspace of $\mathrm{PG}(h(2k+1)-1, p)$ such that $\mathcal{B}(\pi)$ does not correspond to a k-space of $\mathrm{PG}(2k, p^h)$, i.e. if $\mathcal{B}(\pi)$ defines a non-trivial blocking set with respect to k-spaces, then there exists an hk-space π' with $\mathcal{B}(\pi) \cap \mathcal{B}(\pi') = \varnothing$. □

Corollary 4.13. *If $p > 5$ is prime, then there exist minimal double blocking sets with respect to k-spaces in $\mathrm{PG}(2k, p^h)$ of size at most $2\frac{p^{hk+1}-1}{p-1}$.*

5 On the value set of s_{-1} in GF(q^2)

Recall that $k = \gcd(q-2, q^h-1)$ and, by (1),

$$|V(s_{-1})| = q^h - \frac{1}{|D|}\sum_{a\in D}\sigma_0^{\mathcal{U}_0}(a) + \frac{k-1}{k},$$

where $\sigma_0^{\mathcal{U}_0}(a)$ is the number of lines of type (ii) in the parallel class $[a]$ of the affine André plane Π^A that are skew to $\mathcal{U}_0$.

For $a \in D$, let

$$\delta(a) = |\{l \in [a] \colon l \cap \mathcal{U}_0 = \varnothing, l \cap \mathcal{D}_0 \neq \varnothing\}|,$$

and let us write

$$t_0(a) = \sigma_0^{\mathcal{B}_0}(a) = |\{l \in [a] \colon l \cap \mathcal{U}_0 = \varnothing, l \cap \mathcal{D}_0 = \varnothing\}|.$$

Clearly, we have

$$\sigma_0(a) := \sigma_0^{\mathcal{U}_0}(a) = t_0(a) + \delta(a). \tag{2}$$

Let us now consider the case $h = 2$, that is, when Π is a Hall-plane. Then we are in the situation of Lemma 3.8: $\mathcal{B}_0$ is a Baer subplane intersecting ℓ_∞ in one point not in $\mathcal{D}$. We use the notation and the assertions of Lemma 3.9 and Lemma 3.10.

Let ℓ_x be the line $\{(x:0:1) \colon x \in \mathrm{GF}(q^h)\} \cup \{(1:0:0)\}$. As $\mathcal{D}_0 = \mathcal{B}_0 \cap \ell_x$ and $\ell_x \cap \ell_\infty = (1:0:0) \notin \mathcal{D}$, ℓ_x is a line of Π containing $\mathcal{D}_0$, so each line of Π different from ℓ_x contains at most one point of $\mathcal{D}_0$. If $P \in \mathcal{O}^- \cap \mathcal{D}_0$, then every line of type (ii) through P is tangent to $\mathcal{B}_0$, hence skew to $\mathcal{U}_0$. Similarly, if $P \in \mathcal{O} \cap \mathcal{D}_0$ or $P \in \mathcal{O}^+ \cap \mathcal{D}_0$, then there is exactly one or zero line of type (ii) skew to $\mathcal{U}_0$ through P, respectively. Let $\mathcal{L}_\mathcal{O}$ denote the set of lines of type (ii) that are skew to $\mathcal{U}_0$ and intersect $\mathcal{D}_0$ in a point of $\mathcal{O}$. Then $|\mathcal{L}_\mathcal{O}| = |\mathcal{O} \cap \mathcal{D}_0|$ and $\delta(a) = |\mathcal{O}^- \cap \mathcal{D}_0| + |[a] \cap \mathcal{L}_\mathcal{O}|$, whence

$$\sum_{a\in D}\delta(a) = |D| \cdot |\mathcal{O}^- \cap \mathcal{D}_0| + |\mathcal{O} \cap \mathcal{D}_0|.$$

We have that if $k = \gcd(q-2, q^2-1) = \gcd(q-2, 3) = 1$, then $t_0(a) = (q^2-q)/3$ and $\sigma_0(a) = q^2 - |V(s_{-1})|$ are constant on D, hence so is $\delta(a)$. Thus $|\mathcal{O} \cap \mathcal{D}_0| = 0$ or $|\mathcal{O} \cap \mathcal{D}_0| = |D| = q+1$. If q is odd, then $\mathcal{O}$ is an oval of $\mathcal{B}_0$ and only the first case can occur, so $\ell_x \cap \mathcal{B}_0$ is an external line to $\mathcal{O}$, $\delta(a) = |\mathcal{O}^- \cap \mathcal{D}_0| = (q+1)/2$, $\sigma_0(a) = (q^2-q)/3 + (q+1)/2$; consequently, $|V(s_{-1})| = q^2 - (q^2-q)/3 - (q+1)/2$.

If q is even, then $\mathcal{O}$ is a line of $\mathcal{B}_0$ and only the second case can occur, so $\delta(a) = |\mathcal{O}^- \cap \mathcal{D}_0| + 1 = 1$, $\sigma_0(a) = (q^2-q)/3 + 1$; consequently, $|V(s_{-1})| = q^2 - (q^2-q)/3 - 1$. Thus we obtain the following result, which, for q even, was already obtained by Cusick [7].

Theorem 5.1. *Let $q \not\equiv 2 \pmod 3$, and let $s_{-1}\colon x \mapsto x^{-1}(x+1)^{q-1}$ be a function from $\mathrm{GF}(q^2)$ to $\mathrm{GF}(q^2)$, where $0^{-1} = 0^{q^2-2}$ is considered zero. Then the number of elements in the range of s_{-1} is*

$$|V(s_{-1})| = \begin{cases} \frac{2}{3}q^2 - \frac{1}{6}q - \frac{1}{2} & \textit{if } q \textit{ is odd,} \\ \\ \frac{2}{3}q^2 + \frac{1}{3}q - 1 & \textit{if } q \textit{ is even.} \end{cases}$$

Now consider the case $q \equiv 2 \pmod 3$, that is, $k = 3$. Recall that for each $a \in D$, $t_0(a) = q^2 - \frac{2q(q+1)}{3} + \frac{t_2(a)}{3}$ and $\sum_{a\in D} t_2(a) = (q+1)q$. Thus

$$\begin{aligned} \sum_{a\in D} \sigma_0(a) &= \sum_{a\in D}(t_0(a) + \delta(a)) = (q+1)\left(q^2 - \frac{2q(q+1)}{3}\right) + \frac{(q+1)q}{3} + \sum_{a\in D}\delta(a) \\ &= \frac{q(q^2-1)}{3} + (q+1)\cdot|\mathcal{O}^- \cap \mathcal{D}_0| + |\mathcal{O} \cap \mathcal{D}_0|. \end{aligned}$$

Recall that $|D|/k = (q+1)/3$ divides $\sum_{a\in D}\sigma_0(a)$, so $(q+1)/3$ divides $|\mathcal{O} \cap \mathcal{D}_0|$.

Suppose that q is odd. As $\ell_x \cap \ell_\infty \notin \mathcal{D}$, ℓ_x cannot be a tangent to $\mathcal{O}$, hence $|\mathcal{O} \cap \mathcal{D}_0|$ is either 0 or 2. In the latter case, $(q+1)/3 \mid 2$, thus $q = 5$. This case can be handled separately (e.g., by computer), so we assume $q \neq 5$. Then $|\mathcal{O} \cap \mathcal{D}_0| = 0$, so $\ell_x \cap \mathcal{B}_0$ is an external line of $\mathcal{O}$ and $|\mathcal{O}^- \cap \mathcal{D}_0| = (q+1)/2$. Thus

$$\sum_{a\in D}\sigma_0(a) = \frac{q(q^2-1)}{3} + (q+1)\frac{q+1}{2} = \frac{2q^3+3q^2+4q+3}{6}.$$

Now suppose that q is even. Then $|\mathcal{O}\cap\mathcal{D}_0|$ is either 1 or $q+1$, and by $(q+1)/3 \mid |\mathcal{O}\cap\mathcal{D}_0|$, the first case implies $q = 2$ which can be handled separately; thus we may assume $q > 2$ and $|\mathcal{O} \cap \mathcal{D}_0| = q+1$. Then $|\mathcal{O}^- \cap \mathcal{D}_0| = 0$ and

$$\sum_{a\in D}\sigma_0(a) = \frac{q(q^2-1)}{3} + (q+1) = \frac{q^3+2q+3}{3}.$$

Thus we obtain the following result, which, for q even, was already conjectured by Cusick [7] and proved by Rosendahl [16].

Theorem 5.2. *Let $q \equiv 2 \pmod 3$, and let $s_{-1}\colon x \mapsto x^{-1}(x+1)^{q-1}$ be a function from $\mathrm{GF}(q^2)$ to $\mathrm{GF}(q^2)$, where $0^{-1} = 0^{q^2-2}$ is considered zero. Then the number of elements in the range of s_{-1} is*

$$|V(s_{-1})| = \begin{cases} \frac{2}{3}q^2 - \frac{1}{6}q + \frac{1}{6} & \textit{if } q \textit{ is odd,} \\ \\ \frac{2}{3}q^2 + \frac{1}{3}q - \frac{1}{3} & \textit{if } q \textit{ is even.} \end{cases}$$

Acknowledgment

We thank Gordon Royle for his motivating question and Bence Csajbók for his help in finding the papers [7, 16].

References

[1] G. Bacsó, T. Héger, and T. Szőnyi. The 2-blocking number and the upper chromatic number of PG$(2, q)$. *J. Combin. Des.*, 21(12):585–602, 2013.

[2] J. Bamberg, A. Betten, Ph. Cara, J. De Beule, M. Lavrauw, and M. Neunhöffer. *FinInG – Finite Incidence Geometry, Version 1.0*, 2014. http://cage.ugent.be/fining

[3] J. Bierbrauer. Mathematical Reviews MR0695804.

[4] A. Blokhuis, L. Storme, and T. Szőnyi. Lacunary polynomials, multiple blocking sets and Baer subplanes. *J. London Math. Soc. (2)*, 60(2):321–332, 1999.

[5] A. E. Brouwer and A. Schrijver. The blocking number of an affine space. *J. Combinatorial Theory Ser. A*, 24(2):251–253, 1978.

[6] A. A. Bruen and M. J. de Resmini. Blocking sets in affine planes. In *Combinatorics '81 (Rome, 1981)*, volume 18 of *Ann. Discrete Math.*, pages 169–175. North-Holland, Amsterdam-New York, 1983.

[7] T. W. Cusick. Value sets of some polynomials over finite fields GF(2^{2m}). *SIAM J. Comput.*, 27(1):120–131 (electronic), 1998.

[8] T. W. Cusick and P. Müller. Wan's bound for value sets of polynomials. In *Finite fields and applications (Glasgow, 1995)*, volume 233 of *London Math. Soc. Lecture Note Ser.*, pages 69–72. Cambridge Univ. Press, Cambridge, 1996.

[9] J. Eisfeld. On pairs of Baer subplanes in PG$(2, q^2)$. *J. Geom.*, 63(1-2):57–63, 1998.

[10] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.7.8*, 2015. http://www.gap-system.org

[11] J. W. P. Hirschfeld. *Projective geometries over finite fields.* Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, second edition, 1998.

[12] D. R. Hughes and F. C. Piper. *Projective planes.* Springer-Verlag, New York-Berlin, 1973. Graduate Texts in Mathematics, Vol. 6.

[13] R. E. Jamison. Covering finite fields with cosets of subspaces. *J. Combinatorial Theory Ser. A*, 22(3):253–266, 1977.

[14] M. Lavrauw and G. Van de Voorde. Field reduction and linear sets in finite geometry. In *Topics in finite fields*, volume 632 of *Contemp. Math.*, pages 271–293. Amer. Math. Soc., Providence, RI, 2015.

[15] G. Lunardon and O. Polverino. Blocking sets of size $q^t + q^{t-1} + 1$. *J. Combin. Theory Ser. A*, 90(1):148–158, 2000.

[16] P. Rosendahl. On Cusick's method and value sets of certain polynomials over finite fields. *SIAM J. Discrete Math.*, 23(1):333–343, 2008/09.

[17] A. Sonnino. Existence of canonically inherited arcs in Moulton planes of odd order. *Finite Fields Appl.*, 33:187–197, 2015.

[18] T. Szőnyi. Complete arcs in non-Desarguesian planes. *Confer. Sem. Mat. Univ. Bari*, (233):22 pp. (1990), 1989.

[19] T. Szőnyi. Blocking sets in Desarguesian affine and projective planes. *Finite Fields Appl.*, 3(3):187–202, 1997.

[20] T. Szőnyi, A. Gács, and Zs. Weiner. On the spectrum of minimal blocking sets in PG$(2, q)$. *J. Geom.*, 76(1-2):256–281, 2003. Combinatorics, 2002 (Maratea).

[21] T. Szőnyi and Zs. Weiner. Small blocking sets in higher dimensions. *J. Combin. Theory Ser. A*, 95(1):88–101, 2001.