The use of blocking sets in Galois geometries and in related research areas

V. Pepe and L. Storme

Abstract

Blocking sets play a central role in Galois geometries. Besides their intrinsic geometrical importance, the importance of blocking sets also arises from the use of blocking sets for the solution of many other geometrical problems, and problems in related research areas. This article focusses on these applications to motivate researchers to investigate blocking sets, and to motivate researchers to investigate the problems that can be solved by using blocking sets. By showing the many applications on blocking sets, we also wish to prove that researchers who improve results on blocking sets in fact open the door to improvements on the solution of many other problems.

1 Definitions and introductory results

A set B of points of $\mathrm{PG}(n,q)$ is called a *k–blocking set* if every $(n-k)$–dimensional subspace of $\mathrm{PG}(n,q)$ has a non–empty intersection with B, and a set B of points of $\mathrm{PG}(n,q)$ is called a *t–fold* k–blocking set if every $(n-k)$–dimensional subspace contains at least t points of B. In $\mathrm{PG}(2,q)$, the 1–blocking sets are simply called *blocking sets.* Two subspaces Σ_1 and Σ_2 of $\mathrm{PG}(n,q)$ of dimension k and $n-k$ always have a non–empty intersection, hence a set B containing a k–dimensional subspace is called a *trivial* k–blocking set. Moreover, a k–blocking set B is called *minimal* if it is minimal with respect to the containment relation, i.e. $B \setminus \{P\}$ is not a k–blocking set for every $P \in B$, and it is called *small* if $|B| < \frac{3(q^k+1)}{2}$.

The blocking sets of $\mathrm{PG}(2,q)$ have been extensively studied in the last years and there are plenty of results about characterizations (of small ones) and about the bounds on the size. A trivial blocking set of $\mathrm{PG}(2,q)$ is a set of points containing a line. The first examples of non–trivial blocking sets of small size of $\mathrm{PG}(2,q)$ have been given in the following:

Theorem 1. *In $PG(2,q)$, q odd, there exists a projective triangle of side $\frac{q+3}{2}$ that is a minimal blocking set of size $\frac{3(q+1)}{2}$ [14].*

In $PG(2,q)$, q even, there exists a projective triad of side $\frac{q+2}{2}$ that is a minimal blocking set of size $\frac{3q+2}{2}$ [40].

This motivates the choice of the bound $\frac{3(q+1)}{2}$ for the size of a small blocking set in $\mathrm{PG}(2,q)$ and then generalized as $\frac{3(q^k+1)}{2}$ for the k–blocking sets of $\mathrm{PG}(n,q)$.

In $\mathrm{PG}(2,q^2)$, there are other well known examples of minimal blocking sets: the *Baer subplanes* and the *unitals*. A Baer subplane $\mathcal{B}$ of $\mathrm{PG}(2,q^2)$ is a plane isomorphic to $\mathrm{PG}(2,q)$ contained in $\mathrm{PG}(2,q^2)$, hence it has size q^2+q+1 and it has the property that every line of $\mathrm{PG}(2,q^2)$ intersects $\mathcal{B}$ in 1 or $q+1$ points. A unital $\mathcal{U}$ is a set of q^3+1 points of $\mathrm{PG}(2,q^2)$ such that every line of $\mathrm{PG}(2,q^2)$ intersects it in 1 or $q+1$ points and through every point P of $\mathcal{U}$, there exists a unique line ℓ such that $\ell \cap \mathcal{U} = \{P\}$. These two examples are remarkable for the following results:

Theorem 2. *[13] Let B be a non–trivial minimal blocking set of $PG(2,q)$, then $|B| \geq q+\sqrt{q}+1$ and equality holds if and only if q is a square and B is a Baer subplane.*

Theorem 3. *Let B be a minimal blocking set of $PG(2,q)$, then*

- *[15] $|B| \leq q\sqrt{q}+1$,*
- *[16] $|B| = q\sqrt{q}+1$ if and only if q is a square and B is a unital.*

In [8], the following lower bounds for planes of non–square order are proven:

Theorem 4. *If B is a minimal blocking set in $PG(2,q)$ and $q=p^{2h+1}$, p prime, then $|B| \geq q+q^{2/3}+1$ for $p>3$ and $|B| \geq q+q^{2/3}/2^{1/3}+1$ for $p=2,3$.*

On the other hand, there are results about large minimal blocking sets, that are also called *spectrum results*, like the following:

Theorem 5. *[43] There exists a minimal blocking set in $PG(2,q)$, $q>4$, for every size in $[2q-1, 3q-3]$.*

Theorem 6. *[18] For every value k in the interval $[4q\log q, q\sqrt{q}-q+2\sqrt{q}]$, there exists a minimal blocking set of cardinality k in $PG(2,q)$, q square.*

We now list some results about blocking sets in $\mathrm{PG}(n,q)$. We note that most of them are derived from the corresponding planar results. ¿From now on, let θ_k be the number of points of $\mathrm{PG}(k,q)$, that is, $\theta_k = (q^{k+1}-1)/(q-1)$.

Theorem 7. (Bose and Burton [12]) *Let B be a k–blocking set in $\mathrm{PG}(n,q)$ that has the smallest possible cardinality. Then B is a k–dimensional subspace of $\mathrm{PG}(n,q)$.*

Theorem 8. *[5, 36] Let B be a non–trivial k–blocking set in $PG(n,q)$, $q>2$. Then $|B| \geq \theta_k + r(q)q^{k-1}$, where $q+r(q)+1$ is the size of the smallest non–trivial blocking set in $PG(2,q)$, and the equality only holds if B is a cone with base a minimal non–trivial blocking set of size $q+r(q)+1$ of a plane π and vertex a $(k-2)$–dimensional subspace skew to π.*

Theorem 9. *[15, 16] Let B be a minimal 1–blocking set in $PG(n,q)$, $n \geq 3$, then we have the following:*

- *If $n=3$, then $|B| \leq q^2+1$ and the equality holds if and only if B is an ovoid.*
- *If $n \geq 4$, then $|B| < \sqrt{q^{n+1}}+1$.*

Another important result about blocking sets that has been widely used to prove many other theorems is the following:

Theorem 10. *[72] Let B be a small minimal k–blocking set of $PG(n,q)$, $q = p^h$, $p > 2$ prime. Then every subspace that intersects B intersects it in $1 \pmod p$ points.*

In light of this, we define the *exponent* of a small minimal k–blocking set B as the largest integer e for which an $(n-k)$–space intersects B in $1 \pmod{p^e}$ points. Then Sziklai proved:

Theorem 11. *[69] Let B be a small minimal k–blocking set of $PG(n,q)$, $q = p^h$, $p > 2$ prime, with exponent e. Then $e|h$ and every subspace that intersects B in $1 + p^e$ points intersects it in a subline $PG(1,p^e)$.*

Finally, a *Rédei–type* k–blocking set in $\mathrm{PG}(n,q)$ is a blocking set B such that there exists a hyperplane with $|B| - q^k$ points of B. If $|B| < (3q^k+3)/2$, then these k–blocking sets are, in fact, *k–linear blocking sets* (see [3, 67, 73]). A $\mathbb{F}_q$*–linear set* in $\mathrm{PG}(n,q^h)$ is a set of points whose defining vectors form a $\mathbb{F}_q$–vector space (for more details about these sets, see [62]). A k–blocking set B that is also a linear set is called a *linear* k–blocking set. If B, $|B| < (3q^k+3)/2$, is of Rédei–type, then B is linear, but the converse is not true in general (see [60]).

For more results on blocking sets, we refer to the survey articles [6, 71] and also to the chapter on blocking sets [9] in the collected work [23].

The objective of this article is to illustrate the many geometrical problems and problems in related research areas that use blocking sets. The use of blocking sets for solving a great variety of problems gives blocking sets a central place within Galois geometries. By showing the many applications, we wish to motivate researchers to investigate blocking sets, and/or to investigate problems that use blocking sets. We also wish to show to the readers that improved results on blocking sets will imply a large number of improvements to related problems. In particular, in the last section, we state some open problems. One of these open problems is the central problem on blocking sets: the investigation of the linearity conjecture on small (multiple) blocking sets.

To conclude this introduction, we wish to note that p always will denote a prime number and that $\theta_k = (q^{k+1}-1)/(q-1)$ is equal to the number of points in the k–dimensional projective space $\mathrm{PG}(k,q)$ over the finite field $\mathbb{F}_q$ of order q.

We now present a classical example of a problem in Galois geometries that uses blocking sets; the investigation of maximal partial spreads in $\mathrm{PG}(3,q)$ of small deficiency δ.

2 Maximal partial spreads

A *k–spread* $\mathcal{S}$ of the projective space $\mathrm{PG}(n,q)$ is a partition of the point set of $\mathrm{PG}(n,q)$ in k–dimensional subspaces, that is every point of $\mathrm{PG}(n,q)$ is contained in exactly one element of $\mathcal{S}$. It is well known (see e.g. [40]) that such a k–spread exists if and only if $k+1$ divides $n+1$ and then $|\mathcal{S}| = \frac{q^{n+1}-1}{q^{k+1}-1}$. A *partial* k–spread

$\mathcal{S}$ of $\mathrm{PG}(n,q)$ is a collection of pairwise disjoint k–subspaces, that is every point of $\mathrm{PG}(n,q)$ is contained in at most one element of $\mathcal{S}$. A *maximal* partial k–spread is a partial k–spread, maximal with respect to the containment relation. The size of the largest maximal partial k–spread, different from a k–spread, has been investigated in great detail, and this is the classical example of a problem that is investigated, using results on blocking sets.

Let $\mathcal{S}$ be a maximal partial line spread of $\mathrm{PG}(3,q)$ and let $|\mathcal{S}| = q^2 + 1 - \delta$ (a line spread of $\mathrm{PG}(3,q)$ has size q^2+1). We call δ the *deficiency* of $\mathcal{S}$. We will call *holes* the points of $\mathrm{PG}(3,q)$ not contained in any line of $\mathcal{S}$. Since the partial spread is maximal, the set of holes cannot contain lines. Since the lines of $\mathcal{S}$ are pairwise disjoint, every plane contains at most one line of $\mathcal{S}$. The planes containing a line of $\mathcal{S}$ are called *rich*, otherwise they are called *poor*. Let ℓ be a line not in S: the lines of $\mathcal{S}$ meeting ℓ in a point must be contained in distinct planes, hence the number of holes of ℓ is the same as the number of poor planes through ℓ. Let π be a poor plane and let B be the set of holes of π. Every line ℓ of π must contain at least a hole since ℓ is contained in a poor plane. Hence, we have the following:

Lemma 1. *[59] The set of holes of a poor plane of a maximal partial spread of size $q^2 + 1 - \delta$ is a non–trivial blocking set of size $q + \delta$ in this plane.*

Hence, results on non–trivial blocking sets in $\mathrm{PG}(2,q)$ give information on maximal partial spreads in $\mathrm{PG}(3,q)$ of small positive deficiency δ.

Let us first consider q to be a square. The largest value for the size of a blocking set B of $\mathrm{PG}(2,q)$ such that B definitely must contain a Baer subplane has been studied in detail; we list here the best known results. As mentioned in the preceding section, p will always denote a prime number.

Theorem 12. *Let B be a non–trivial blocking set of $PG(2,q)$, q square.*

1. *[8] Let $q = p^h, h > 2$, $c_2 = c_3 = 2^{-\frac{1}{3}}$ and $c_p = 1$ for $p > 3$. If $|B| < q + c_p q^{\frac{2}{3}} + 1$, then B contains a Baer subplane.*
2. *[70] Let $q = p^2$. If $|B| < 3(q+1)/2$, then B contains a Baer subplane.*

In general, let $\delta(q)$ be the maximum integer such that a non–trivial blocking set of $\mathrm{PG}(2,q)$ of size $q + \delta(q)$ must contain a Baer subplane. Then, for every maximal partial spread $\mathcal{S}$ of positive deficiency $\delta \leq \delta(q)$, the set of holes in a poor plane of $\mathcal{S}$ contains a Baer subplane of holes. One might wonder where all these Baer subplanes of holes in these poor planes arise from. A logical guess would be that the set of holes is the union of Baer subgeometries $\mathrm{PG}(3,\sqrt{q})$, since $|\mathrm{PG}(3,\sqrt{q})| = (\sqrt{q}+1)(q+1) \equiv 0 \pmod{q+1}$. This indeed was proven. Using the results about blocking sets, in [59], the following theorem was proven.

Theorem 13. *Let $q > 4$ be a square, let $\delta(q)$ be defined as before, $0 < \delta \leq \min\{(q+1)/2, \delta(q)\}$. If $\mathcal{S}$ is a maximal partial spread of size $q^2 + 1 - \delta$, then*

a) *$\delta = s(\sqrt{q}+1)$ for some integer $s \geq 2$,*

b) *the set of holes of $PG(3,q)$ is the union of s pairwise disjoint Baer subgeometries $PG(3,\sqrt{q})$.*

However, it is important to mention that no examples of maximal partial spreads in $\mathrm{PG}(3,q)$ having a set of holes equal to the union of $\sqrt{q}-1 > s > 1$ pairwise disjoint Baer subgeometries $\mathrm{PG}(3,\sqrt{q})$ are known. Most likely, such maximal partial spreads do not exist. The proof of the (non–)existence of such maximal partial spreads is one of the open problems we mention in Subsection 7.5.

Let us now consider maximal partial spreads in $\mathrm{PG}(3,q^3)$, where $q=p^h$, h odd, $p \geq 7$.

Under these hypotheses for q, the non–trivial minimal blocking sets of $\mathrm{PG}(2,q^3)$ of the smallest and second smallest size have been completely classified in [7, 61, 63, 70].

Theorem 14. *In $PG(2,q^3)$, $q=p^h$, $p \geq 7$, h odd, p prime, the smallest and the second smallest sizes for a non–trivial minimal blocking set are q^3+q^2+1 and q^3+q^2+q+1, respectively. The minimal blocking sets of these sizes are unique up to projective equivalence and they are of Rédei type. More precisely, they are projected subgeometries $PG(3,q)$ in a plane $PG(2,q^3)$.*

Similarly, as for q square, the set of holes in a poor plane $\mathrm{PG}(2,q^3)$, $q = p^h$, $p \geq 7$, h odd, p prime, of a maximal partial spread, of deficiency $\delta \leq q^2+q+1$, contains a projected subgeometry $\mathrm{PG}(3,q)$. Again, where can all these projected subgeometries $\mathrm{PG}(3,q)$ of holes arise from? A logical guess is a projected subgeometry $\mathrm{PG}(5,q)$ in $\mathrm{PG}(3,q^3)$ of size $q^5+q^4+q^3+q^2+q+1 = (q^2+q+1)(q^3+1) \equiv 0 \pmod{q^3+1}$. This was indeed proven to be the case.

Theorem 15. *[59] Let $\mathcal{S}$ be a maximal partial spread of size $q^6+1-\delta$ of $PG(3,q^3)$, where $q=p^h$, h odd, $p \geq 7$, p prime, $0 < \delta \leq q^2+q+1$. Then $\delta = q^2+q+1$ and the set of holes forms a projected subgeometry $PG(5,q)$ in $PG(3,q^3)$.*

Finally, let $\mathcal{S}$ be a maximal partial spread of $\mathrm{PG}(3,q^3)$, where $q=p^h$, $h \geq 2$ even, $p \geq 7$. Combining the aforementioned results, it is possible to describe the set of holes of $\mathcal{S}$ when its deficiency is small. As before, we first state the results on the small minimal non–trivial blocking sets of the plane.

Theorem 16. *[63] In $PG(2,q^3)$, where $q=p^h$, $h \geq 2$ even, $p \geq 7$, the smallest non–trivial blocking sets are:*

a) *a Baer subplane $PG(2,q^{\frac{3}{2}})$ (hence of order $q^3+q^{\frac{3}{2}}+1$);*

b) *a minimal blocking set of Rédei type of size q^3+q^2+1 which is a projected subgeometry $PG(3,q)$;*

c) *a minimal blocking set of Rédei type of size q^3+q^2+q+1 which is a projected subgeometry $PG(3,q)$.*

Theorem 17. *Let $\mathcal{S}$ be a maximal partial spread of size $q^6+1-\delta$ of $PG(3,q^3)$, where $q=p^h$, h even, $p \geq 7$, $0 < \delta \leq q^2+q+1$. If there is a Baer subplane of holes, then all poor planes contain a Baer subplane of holes, $\delta = s(q^{\frac{3}{2}}+1)$, $s \geq 2$, and the set of holes is the union of s pairwise disjoint subgeometries $PG(3,q^{\frac{3}{2}})$.*

If no poor plane contains a Baer subplane of holes, then $\delta = q^2+q+1$ and the set of holes forms a projected subgeometry $PG(5,q)$ in $PG(3,q^3)$.

It is clear from the preceding results that improved characterization results on small minimal non–trivial blocking sets in $\mathrm{PG}(2,q)$ will imply improved characterization results on maximal partial spreads of small positive deficiency δ.

We refer to [5, 28] for a more general application of the results about blocking sets in order to find a lower bound on the size of maximal partial t–spreads in $\mathrm{PG}(n,q)$. Precisely, let $\mathcal{S}$ be a maximal partial t–spread of $\mathrm{PG}(n,q)$: the maximality of $\mathcal{S}$ implies that the set of points contained in an element of $\mathcal{S}$ is an $(n-t)$–blocking set of $\mathrm{PG}(n,q)$. In [28], the author constructs as follows small maximal partial t–spreads: let B be a minimal $(n-t)$–blocking set of $\mathrm{PG}(n,q)$, then try to find a partial t–spread $\mathcal{S}_1$ that contains as many points of B as possible; let A be $B \setminus \mathcal{S}_1$, then try to find the smallest set $\mathcal{S}_2$ of mutually disjoint t–spaces that covers all the points of A. In the same paper, the author finds a construction for maximal partial t–spreads:

Theorem 18. *In $PG(n,q)$, $n = k(t+1)+t-1+r$, with $k \geq 2$, there exist maximal partial t–spreads of size*

$$q^r \frac{q^{k(t+1)}-1}{q^{t+1}-1} + q^\beta - q^r + 1, \ \textit{where} \left\{ \begin{array}{ll} \beta = -\infty & \textit{if } r = 0, \\ \beta = \lceil (t+r-1)/2 \rceil + 1 & \textit{otherwise.} \end{array} \right. \quad (1)$$

Hence, by *small* maximal partial t–spreads, we mean maximal partial t–spreads of size less than (1). As stated in Section 1, the smallest minimal $(n-t)$–blocking set of $\mathrm{PG}(n,q)$ is a trivial one, i.e. an $(n-t)$–space, and the second smallest one is given by Theorem 8. By counting arguments, it is easy to see that if B is a blocking set as described in Theorem 8, a set of t–spaces covering $|B|$ points has size larger than (1), hence to find lower bounds on small maximal partial t–spreads, it is necessary to start from an $(n-t)$–space; in this way it is possible to find the following bounds:

Theorem 19. *[28] In $PG(n,q)$, $n = k(t+1)+t-1+r$, with $k \geq 2$, let $\mathcal{S}$ be a smallest maximal partial t–spread. Then the following hold:*

- *if $r = 0$, then $|\mathcal{S}| = \frac{q^{k(t+1)}-1}{q^{t+1}-1}$ (this is actually proven in [5]);*
- *if $r = 1$, then $|\mathcal{S}| \geq q\frac{q^{k(t+1)}-1}{q^{t+1}-1} + q^2 - q + 1$;*
- *if $r > 1$ and $t+1 \geq 2r$, then $|\mathcal{S}| \geq q^r \frac{q^{k(t+1)}-1}{q^{t+1}-1} + (q^{r+1} - q^r)/2 + 1$;*
- *if $r > 1$ and $t+1 < 2r$, then $|\mathcal{S}| \geq q^r \frac{q^{k(t+1)}-1}{q^{t+1}-1} + (q^{r+1} - q^r + q^{2r-t-1} + 3q + 1)/2$.*

In some cases, these lower bounds and the upper bound given by (1) coincide and so we have the exact size of a smallest maximal partial t–spread:

Corollary 1. a) *In $PG(2k+1,q)$, $k \geq 2$, the smallest maximal partial line spreads have size $q\frac{q^{2k}-1}{q^2-1} + q^2 - q + 1$.*

b) *In $PG(3k+2,q)$, $k \geq 2$, the smallest maximal partial plane spreads have size $q\frac{q^{3k}-1}{q^3-1} + q^2 - q + 1$.*

3 Blocking sets and coding theory

The most natural application of finite geometry to coding theory occurs when the codes are *linear*. Let $\mathbb{F}_q$ be the finite field of order q and let $V := \mathbb{F}_q^n$ be the n–dimensional vector space of the n–tuples over $\mathbb{F}_q$. A linear code C is a k–dimensional subspace of V and it is called an $[n, k]$ *code* over $\mathbb{F}_q$ or an $[n, k]_q$ code. The *Hamming distance* $d(c, c')$ of two codewords c and c' is the number of the components in which they differ and the *minimum distance* d of C is the minimum of the set $\{d(c, c')|c, c' \in C, c \neq c'\}$. A linear $[n, k]$ code or $[n, k]_q$ code having minimum distance d is denoted by $[n, k, d]$ *code* or $[n, k, d]_q$ *code*. The *weight* $w(c)$ of a codeword c is the number of the non–zero components of c. It is well known (see for example [37]) that for a linear code C, $\min\{w(c)|c \in C\backslash\{\mathbf{0}\}\} = \min\{d(c, c')|c, c' \in C, c \neq c'\}$. One of the main reasons why the weight of the codewords of a linear code is investigated is that a code C with minimum distance d can correct up to t errors, where $2t + 1 \leq d$.

One of the ways to define a linear code C is by means of its generator matrix H. If H is the incidence matrix of a finite geometry, the properties of the geometries can be translated to properties of C and we have in this case powerful tools to investigate the minimum distance and the weight distribution of C. If H is the incidence matrix of the points and k–spaces of $\mathrm{PG}(n, q)$, then we will denote the code generated by H by $C_k(n, q)$. When we say that a vector $v \in C_k(n, q)$ is a subset S of $\mathrm{PG}(n, q)$, we mean that v is the incidence vector of S. We let (c_1, c_2) denote the scalar product in $\mathbb{F}_q$ of two codewords c_1 and c_2 of a q–ary linear code C. The *dual code* $C^\perp$ of a q–ary linear code C of length m is the set of all vectors orthogonal to all the codewords of C, hence $C^\perp = \{v \in V(m, q)|(v, c) = 0, \forall c \in C\}$. If C is a linear $[m, k]$–code, then $C^\perp$ is an $[m, m - k]$–code and if H is a generator matrix for C, then H is a parity check matrix for $C^\perp$. Hence, $C_k(n, q)^\perp$ is the code that has as parity check matrix H the incidence matrix of points and k–dimensional spaces of $\mathrm{PG}(n, q)$. The minimum distance d of $C_k(n, q)^\perp$ satisfies the following inequality ([17]): $(q + p)q^{n-k-1} \leq d \leq 2q^{n-k}$, where $q = p^h$, and for $p = 2$, the lower bound is sharp. In [49], the authors use some properties of blocking sets to prove upper bounds on $d(C_k(n, q)^\perp)$.

Theorem 20. *[49] Let B be a minimal $(n - k)$–blocking set in $PG(n, q)$ of size $q^{n-k} + x$, with $x < (q^{n-k} + 3)/2$, such that there exists an $(n - k)$–space μ intersecting B in x points. The difference of the incidence vectors of B and μ is a codeword of $C_k(n, q)^\perp$ with weight $2q^{n-k} + \theta_{n-k-1} - x$.*

Theorem 21. *[49] There exists a small minimal $(n - k)$–blocking set B of size $q^{n-k} + x$ in $PG(n, q)$, $q = p^h$, such that there is an $(n - k)$–space μ with $|B \cap \mu| = x$ and with $x = q^{n-k-1}(q - 1)/(p - 1) + \theta_{n-k-2}$.*

Corollary 2. *[49] The minimum weight d of $C_k(n, q)^\perp$ satisfies the following inequality: $d \leq 2q^{n-k} - q^{n-k-1}(q - p)/(p - 1)$.*

There are also applications of the theory of the blocking sets to the study of the weights of the codewords of $C_k(n, q)$. To define $C_k(n, q)$, we have considered the incidence matrix H, that is we have labeled the columns of H by the points of $\mathrm{PG}(n, q)$, hence we have ordered the points. Let $c \in C_k(n, q)$ and let *supp*(c) be the set of indices i for which the ith–component of c is non–zero: this set defines a set S of points of $\mathrm{PG}(n,q)$ and we will say that S is defined by c. As a first application, we mention the following theorem:

Theorem 22. *[1] The minimum weight of $C_k(n,q)$ is θ_k and a codeword of such a weight is a scalar multiple of the incidence vector of a k–space.*

This can be proven in an easy way (see [73, Theorem 6.3.3]) using the fact that a small weight codeword defines a k–blocking set and using the well known result that a k–blocking set of $\mathrm{PG}(n,q)$ of size θ_k is a k–space (Theorem 7). Moreover, using the link between k–blocking sets and the codewords of $C_k(n,q)$, it is possible to compute a gap for the weight of the codewords. The first useful result is the following:

Lemma 2. *[51] Let $c \in C_k(n,q)$, then there exists a value $a \in \mathbb{F}_p$ such that $(c,\mu) = a$ for all the subspaces μ of $PG(n,q)$ of dimension at least $n-k$.*

Then it is easy to prove the following.

Theorem 23. *Let $c \in C_k(n,q)$, $q = p^h$, $p > 3$, with $w(c) < 2q^k$, such that $(c,\mu) \neq 0$ for some $(n-k)$–space μ, then c is a scalar multiple of the incidence vector of a small minimal k–blocking set in $PG(n,q)$.*

Moreover, it is useful to see how the set defined by a codeword intersects a given blocking set.

Lemma 3. *[51] Let $c \in C_k(n,q)$, $q = p^h$, $p > 3$, with $w(c) < 2q^k$, such that $(c,\mu) \neq 0$ for some $(n-k)$–space μ, and let B be a small minimal $(n-k)$–blocking set. Then the set S of points defined by c intersects B in $1 \bmod p$ points.*

This very strong condition led to the following result about blocking sets.

Theorem 24. *[51] If B is a minimal k–blocking set in $PG(n,p^h)$, $p > 2$, $|B| \leq 3(p^{hk} - p^{hk-1})/2$, intersecting every $\mathbb{F}_p$–linear $(n-k)$–blocking set in $1 \bmod p$ points, then B is trivial.*

By Lemma 2, we have that either $(c,\mu) \neq 0$ for all $(n-k)$–spaces μ, or $(c,\mu) = 0$ for all $(n-k)$–spaces μ, but in the latter case we get $c \in C_k(n,q)^\perp$. If $c \notin C_k(n,q)^\perp$ and $w(c) < 2q^k$, then by Theorem 23 we have that $supp(c)$ defines a small minimal k–blocking set B that by Lemma 3 and Theorem 24 turns out to be trivial, that is B is a k–subspace and $w(c) = \theta_k$. Hence, we have the following theorem.

Theorem 25. *[51] There are no codewords in $C_k(n,q) \setminus C_k(n,q)^\perp$, $p > 5$, with weight in the interval $]\theta_k, 2q^k[$.*

Finally, since we have:

Theorem 26. *[2] The minimum weight for $C_k(n,q)^\perp$ is at least $2(\frac{q^n-1}{q^{n-k}-1}(1-\frac{1}{p})+\frac{1}{p})$.*

We get the following gap for the weight of the codewords of $C_k(n,q)$.

Theorem 27. *[51] There are no codewords in $C_k(n,q)$, $p > 5$, with weight in the interval $]\theta_k, 2(\frac{q^n-1}{q^{n-k}-1}(1-\frac{1}{p})+\frac{1}{p})[$.*

4 Minihypers and the Griesmer bound

4.1 The Griesmer bound

The Griesmer bound in coding theory gives a lower bound on the length n of a k–dimensional linear code over the finite field $\mathbb{F}_q$ of order q, having minimum distance d.

Theorem 28. ([32, 64]) *For every linear* $[n, k, d]_q$ *code,*

$$n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil = g_q(k, d),$$

where $\lceil x \rceil$ *denotes the smallest integer larger than or equal to* x.

Linear codes attaining the Griesmer bound, i.e. with parameters $[g_q(k, d), k, d]_q$, are called *Griesmer codes.*

The problem of whether the lower bound $g_q(k, d)$ is sharp for given k, d, and q is a difficult problem. This problem is investigated by many different techniques, one of which uses the geometrical concept of *minihypers.*

We now give the definition of a minihyper, as stated in the literature, but as immediately can be seen from the definition, a minihyper is nothing else than a blocking set. In the following definition, a multiset $(\mathcal{H}, w)$ in $\mathrm{PG}(N, q)$ is a set of points $\mathcal{H}$ of $\mathrm{PG}(N, q)$ with a weight function w associating a non–negative integer to every point P of $\mathrm{PG}(N, q)$.

Definition 1. *A multiset* (F, w) *in* $\mathrm{PG}(N, q)$ *is called an* $(f, m; N, q)$–minihyper *if*

(a) $P \in F \Longleftrightarrow w(P) > 0$;

(b) $\displaystyle\sum_{P \in \mathrm{PG}(N,q)} w(P) = f$;

(b) $|F \cap H| = \displaystyle\sum_{P \in F \cap H} w(P) \geq m$ *for any hyperplane* H*, and there exists a hyperplane* H_0 *with* $|F \cap H_0| = m$.

In case $w(P) \in \{0, 1\}$ *for every point* P *of* $PG(N, q)$*, we can omit the weight function* w *in the definition of the minihyper and simply denote the minihyper by* F*, and refer to it as* projective minihyper*. We will also speak of* (f, m)–minihypers *if the geometry* $\mathrm{PG}(N, q)$ *we consider is clear from the context.*

It is immediately clear from the definition that an $(f, m; N, q)$–minihyper is in fact an m–fold 1–blocking set of size f. So, in the definition of an $(f, m; N, q)$–minihyper, not only the minimal number m of points the set has in common with every hyperplane is of importance, also the exact size f of the $(f, m; N, q)$–minihyper is of importance.

The reason why both the size f and the minimal number m of points the minihyper has in common with every hyperplane are important follows from the close link between linear codes meeting the Griesmer bound and their geometrical counterpart of the minihypers.

We now describe this link and a general class of minihypers.

4.2 Minihypers and the Belov-Logachev-Sandimirov construction

The link between minihypers in $\mathrm{PG}(k-1,q)$ and linear $[n,k,d]_q$ codes meeting the Griesmer bound is described in the following way.

For $(s-1)q^{k-1} < d \leq sq^{k-1}$, d can be written uniquely as $d = sq^{k-1} - \sum_{i=1}^{h} q^{\lambda_i}$ such that:

(a) $0 \leq \lambda_1 \leq \cdots \leq \lambda_h < k-1$,

(b) at most $q-1$ of the values λ_i are equal to a given value.

Using this expression for d, the Griesmer bound for a linear $[n,k,d]_q$ code becomes:

$$n \geq s\theta_{k-1} - \sum_{i=1}^{h} \theta_{\lambda_i}.$$

Hamada and Helleseth showed that in the case $d = sq^{k-1} - \sum_{i=1}^{h} q^{\lambda_i}$, there is a one–to–one correspondence between the set of all non–equivalent $[n,k,d]_q$ codes meeting the Griesmer bound and the set of all projectively distinct $(\sum_{i=1}^{h} \theta_{\lambda_i}, \sum_{i=1}^{h} \theta_{\lambda_i - 1}; k-1, q)$–minihypers $\mathcal{F}$ [34]. This correspondence is as follows:

Consider a generator matrix $G = (P_1 \cdots P_n)$ of the $[n,k,d]_q$ code C meeting the Griesmer bound, and let $(s-1)q^{k-1} < d \leq sq^{k-1}$, where d is written as $d = sq^{k-1} - \sum_{i=1}^{h} q^{\lambda_i}$, described above. Then the n columns of G define points of the projective space $\mathrm{PG}(k-1,q)$. Consider the multiset $s \cdot \mathrm{PG}(k-1,q)$, which is equal to s copies of the projective space $\mathrm{PG}(k-1,q)$. Then the multiset $s \cdot \mathrm{PG}(k-1,q) \setminus \{P_1, \ldots, P_n\}$ is equal to a $(\sum_{i=1}^{h} \theta_{\lambda_i}, \sum_{i=1}^{h} \theta_{\lambda_i - 1}; k-1, q)$–minihyper $(\mathcal{F}, w)$. In other words, the weight w of a point P of $\mathrm{PG}(k-1,q)$ is equal to s minus the number of columns of G defining the point P of $\mathrm{PG}(k-1,q)$. Alternatively, the minihyper corresponding to a Griesmer code is the multiset in $s \cdot \mathrm{PG}(k-1,q)$ obtained by taking the complement of the multiset $\{P_1, \ldots, P_n\}$ in the multiset $s \cdot \mathrm{PG}(k-1,q)$.

We note that this construction of linking minihypers to Griesmer codes is also known in the literature under the name of *anticodes* [58].

Belov, Logachev, and Sandimirov [4] gave a construction method for Griesmer codes, which is easily described by using the corresponding minihypers.

Consider in $\mathrm{PG}(k-1,q)$ a sum of ϵ_0 points $P_1, P_2, \ldots, P_{\epsilon_0}$, ϵ_1 lines $\ell_1, \ell_2, \ldots, \ell_{\epsilon_1}$, $\ldots$, ϵ_{k-2} $(k-2)$–dimensional subspaces $\pi_1^{(k-2)}, \ldots, \pi_{\epsilon_{k-2}}^{(k-2)}$, with $0 \leq \epsilon_i \leq$

$q-1, i=0,\ldots,k-2$, then such a sum defines a $(\sum_{i=0}^{k-2}\epsilon_i\theta_i, \sum_{i=0}^{k-2}\epsilon_i\theta_{i-1}; k-1, q)$–minihyper $\mathcal{F}$, where the weight of a point R of PG$(k-1,q)$ *equals the number of objects, in the description above, in which it is contained.*

Now that the standard examples of minihypers are known, different problems on minihypers arise. One of them is the construction of other examples of minihypers. The Belov-Logachev-Sandimirov construction can be extended by allowing subgeometries and projected subgeometries, but there must be definitely many other types of minihypers. There is also the problem of determining the minihypers which cannot be written as the sum of two other smaller minihypers. One of the problems investigated greatly in recent years is the characterization problem on minihypers, and equivalently on linear codes meeting the Griesmer bound:

Characterize $(f,m;k-1,q)$–minihypers $\mathcal{F}$ for given parameters $f=\sum_{i=0}^{k-2}\epsilon_i\theta_i$, $m=\sum_{i=0}^{k-2}\epsilon_i\theta_{i-1}$, k, and q.

Fundamental research on this problem was performed by Hamada *et al* who, in many articles, obtained a lot of results on minihypers and who developed a great amount of techniques useful in the study of minihypers. Their main results are in [33, 35].

Since the research they performed, the techniques they developed have been extended, including the use of the recent results on blocking sets. This has made it possible to obtain great improvements. Since minihypers are in fact particular blocking sets, the complete characterization of minihypers is greatly based on corresponding characterization results on blocking sets. However, differences occur between the geometrical study of blocking sets, and the corresponding coding–theoretical characterizations of minihypers.

The geometrical interest is mainly the characterization of minimal blocking sets. This characterization includes minimal blocking sets which are cones having a vertex and a base which is a non–trivial minimal blocking set in a smaller space. But such cones are not always minihypers with the correct parameters $(\sum_{i=1}^{h}\theta_{\lambda_i}, \sum_{i=1}^{h}\theta_{\lambda_i-1}; k-1, q)$. For instance, consider a 2–blocking set B in PG$(3,q)$, q square, which is a cone with vertex the point P and base the Baer subplane PG$(2,\sqrt{q})$ in a plane skew to P. This cone has size $f=q^2+q\sqrt{q}+q+1$, and it intersects every plane in at least $m=\sqrt{q}+1$ points. But it is not possible to write (f,m) in the form $(\sum_{i=1}^{h}\theta_{\lambda_i}, \sum_{i=1}^{h}\theta_{\lambda_i-1})$. For the main known results on minihypers, we refer to the survey articles [65, 66] and also to the chapter on *Galois geometries and coding theory* [46] that appeared in the collected work *Recent research topics in Galois geometry* [23].

We mention here the most recent results on projective minihypers, and on weighted minihypers.

Theorem 29. (De Beule, Metsch, and Storme [22]) *A projective* $(\sum_{i=0}^{k-2} \epsilon_i\theta_i, \sum_{i=0}^{k-2} \epsilon_i\theta_{i-1}; k-1, q)$*–minihyper, where* $\sum_{i=0}^{k-2} \epsilon_i \leq \delta_0$ *with* δ_0 *equal to one of the values in Table* 4.1*, is a union of* ϵ_{k-2} *hyperplanes,* ϵ_{k-3} $(k-3)$*–dimensional spaces,* $\ldots, \epsilon_1$ *lines, and* ϵ_0 *points, which all are pairwise disjoint, so is of Belov-Logachev-Sandimirov type.*

In the following table, $q = p^s$, p prime, $s \geq 1$.

p	s	δ_0
p	1	$\leq (p+1)/2$
p	3	$\leq p^2$
p	even	$\leq \sqrt{q}$
2	$6m+1, m \geq 1$	$\leq 2^{4m+1} - 2^{4m} - 2^{2m+1}/2$
> 2	$6m+1, m \geq 1$	$\leq p^{4m+1} - p^{4m} - p^{2m+1}/2 + 1/2$
2	$6m+3, m \geq 1$	$< 2^{4m+5/2} - 2^{4m+1} - 2^{2m+1} + 1$
> 2	$6m+3, m \geq 1$	$\leq p^{4m+2} - p^{2m+2} + 2$
≥ 5	$6m+5, m \geq 0$	$< p^{4m+7/2} - p^{4m+3} - p^{2m+2}/2 + 1$

Table 4.1: Upper bounds on δ_0

Theorem 30. (De Beule, Metsch, and Storme [21]) *A* $(\sum_{i=0}^{k-2} \epsilon_i\theta_i, \sum_{i=0}^{k-2} \epsilon_i\theta_{i-1};$ $k-1, q)$*–minihyper, where* $\sum_{i=0}^{k-2} \epsilon_i < \sqrt{q}+1$*, is a sum of* ϵ_{k-2} *hyperplanes,* ϵ_{k-3} $(k-3)$*–dimensional spaces,* $\ldots, \epsilon_1$ *lines, and* ϵ_0 *points, so it is of Belov-Logachev-Sandimirov type.*

The results on the minihypers are obtained by using results on blocking sets via different kinds of methods.

For instance, consider a $(\sum_{i=0}^{s} \epsilon_i\theta_i, \sum_{i=0}^{s} \epsilon_i\theta_{i-1}; k-1, q)$–minihyper F, $\sum_{i=0}^{s} \epsilon_i = h$ small and with $\epsilon_s \neq 0$. Then there exist $(k-s)$–dimensional subspaces Π_{k-s} intersecting F in $(\epsilon_s(q+1)+m_0^{(s-1)}, \epsilon_s; k-s, q)$–minihypers, with $\epsilon_s+m_0^{(s-1)} \leq h$. This is in fact an ϵ_s–fold 1–blocking set in Π_{k-s}. If these ϵ_s–fold 1–blocking sets in PG$(k-s, q)$ are characterized, then the $(k+1-s)$–dimensional spaces Π_{k+1-s} intersecting F in $(\epsilon_s(q^2+q+1)+\epsilon_{s-1}(q+1)+m_0^{(s-2)}, \epsilon_s(q+1)+\epsilon_{s-1}; k+1-s, q)$–minihypers F_{k+1-s}, with $\epsilon_s+\epsilon_{s-1}+m_0^{(s-2)} \leq h$, can sometimes be characterized via the many hyperplanes of Π_{k+1-s} that intersect F in $(\epsilon_s(q+1)+m_0^{(s-1)}, \epsilon_s; k-s, q)$–minihypers, with $\epsilon_s + m_0^{(s-1)} \leq h$.

Inductively, if all the $(\sum_{i=j+1}^{s} \epsilon_i\theta_{i-j} + m_0^{(j)}, \sum_{i=j+1}^{s} \epsilon_i\theta_{i-j-1}; k-1-j, q)$–minihypers, with $\sum_{i=j+1}^{s} \epsilon_i + m_0^{(j)} \leq h$, are characterized, then sometimes all the

$(\sum_{i=j}^{s} \epsilon_i\theta_{i+1-j} + m_0^{(j-1)}, \sum_{i=j}^{s} \epsilon_i\theta_{i-j}; k-j, q)$–minihypers, with $\sum_{i=j}^{s} \epsilon_i + m_0^{(j-1)} \leq h$, can be characterized. Finally, for $j = 0$, this might lead to the complete characterization of the $(\sum_{i=0}^{s} \epsilon_i\theta_i, \sum_{i=0}^{s} \epsilon_i\theta_{i-1}; k-1, q)$–minihypers F, with $\sum_{i=0}^{s} \epsilon_i = h$.

For instance, this method was used in [21, 22] and in [33, 35].

Since the characterization of minihypers heavily relies on the characterization results on (multiple) blocking sets in the plane $\mathrm{PG}(2, q)$, also here we have the phenomenon that improved characterization results on (multiple) blocking sets in $\mathrm{PG}(2, q)$ imply improved characterization results on minihypers.

5 Extension results

Recently, a new link of blocking sets to a coding-theoretical problem has been found. Namely, a link between blocking sets and the extendability of linear codes has been determined. This link has already been used in combination with the two classical results on blocking sets of Bose-Burton (Theorem 7) and of Beutelspacher-Heim (Theorem 8).

Regarding the extendability problem for linear codes, it is already known for a long time that a binary $[n, k, d]$ code of odd minimum distance d can be extended to an $[n + 1, k, d + 1]$ code by adding a parity check. This result has been generalized by Hill and Lizak in [38, 39].

Theorem 31. (Hill and Lizak [38, 39]) *Let C be an $[n, k, d]_q$ code with $\gcd(d, q) = 1$ and with all non–zero weights congruent to 0 or $d \pmod q$. Then C can be extended to an $[n + 1, k, d + 1]_q$ code.*

The geometrical version of this result is obtained in the following way. For the details, we refer to the chapter on Galois geometries and coding theory [46] in the collected work [23].

Consider a generator matrix $G = (P_1 \cdots P_n)$ of the linear code C of Theorem 31. Then the n columns of G define an $(n, w; k - 1, q)$–arc, i.e., a multiset of n points in $\mathrm{PG}(k-1, q)$ intersecting every hyperplane in at most $w = n-d$ points, and with moreover $\gcd(n - w, q) = 1$. ¿From the assumptions of Theorem 31, the intersection sizes of all hyperplanes with this multiset are congruent to n or $w \pmod q$.

A geometrical proof shows that there are $(q^{k-1} - 1)/(q - 1)$ hyperplanes with intersection size congruent to $n \pmod q$, which form a dual blocking set with respect to the $(k - 3)$–dimensional subspaces of $\mathrm{PG}(k - 1, q)$, i.e., through every $(k - 3)$–dimensional subspace of $\mathrm{PG}(k - 1, q)$, there passes at least one hyperplane of $\mathrm{PG}(k-1, q)$ with intersection size congruent to $n \pmod q$. By the dual of the Bose-Burton theorem (Theorem 7), these hyperplanes pass through a fixed point P. Hence, we can construct an $(n+1, w; k-1, q)$–arc by increasing the multiplicity of P by 1.

Then $\hat{G} = (P_1 \cdots P_nP)$ is the generator matrix of an $[n + 1, k, d + 1]_q$ code $\hat{C}$ which is an extension of C.

Using the result of Beutelspacher and Heim (Theorem 8) and the geometrical ideas described above, the preceding result was improved.

Theorem 32. (Landjev and Rousseva [45]) *Let $\mathcal{K}$ be an $(n, w; k-1, q)$–arc, $q = p^s$, with spectrum $(a_i)_{i \geq 0}$. Let $w \not\equiv n \pmod{q}$ and*

$$\sum_{i \not\equiv w \pmod{q}} a_i < q^{k-2} + q^{k-3} + \cdots + q + 1 + q^{k-3} \cdot r(q), \qquad (2)$$

where $q + r(q) + 1$ is the minimal size of a non–trivial blocking set of $\mathrm{PG}(2, q)$*. Then $\mathcal{K}$ is extendable to an $(n+1, w; k-1, q)$–arc.*

This result is as follows restated into a non–extendability result for linear codes.

Theorem 33. *Let C be a non–extendable $[n, k, d]_q$ code, $q = p^s$, with* $\gcd(d, q) = 1$*. If $(A_i)_{i \geq 0}$ is the spectrum of C, then $\sum_{i \not\equiv 0, d \pmod{q}} A_i \geq q^{k-3} \cdot r(q)$, where $r(q)$ is the same as in Theorem 32.*

6 Blocking sets and cryptography

We now mention an application of blocking sets in cryptography.

In [44], the authors designed a new key distribution scheme for TV–nets. A major problem in the design of such a key distribution scheme is the fact that sometimes subscribers to such a TV–net become compromised; this means that they no longer wish to pay for receiving the programs of this latter TV–net. If this happens, the codes (called *keys*) of these compromised subscribers become themselves compromised, and must be no longer valid. The system of [44], based on points and lines of projective planes, enables a TV–net to distribute keys to their subscribers in such a way that keys still remain valid, even if subscribers become compromised. Only if certain subsets of compromised subscribers are reached, the TV–net has to distribute a new set of keys to all of their subscribers. We now describe this key distribution scheme.

We identify the subscribers with the points of a projective plane $\mathrm{PG}(2, q)$. The keys are identified with the lines of the projective plane $\mathrm{PG}(2, q)$.

If a person subscribes to the TV–net, he is identified with a point P of $\mathrm{PG}(2, q)$ and he receives the keys of all the lines of $\mathrm{PG}(2, q)$ passing through P. This enables him to receive the programs of the TV–net.

If however a subscriber P decides not to pay any longer for receiving the programs of the TV–net, the keys of the lines of $\mathrm{PG}(2, q)$ passing through the point P become invalid. This is no problem for the other subscribers since they still lie on q lines not passing through P, so they still have q valid keys for receiving the programs of the TV–net.

It is clear that if at most q subscribers become compromised, then every non–compromised subscriber still has at least one valid key to receive the programs of the TV–net. More precisely, when does a non–compromised subscriber Q loose all his keys to view the programs? He looses all keys when all the keys of the lines of $\mathrm{PG}(2, q)$ through Q become invalid. In other words, when the set of compromised subscribers forms a trivial dual blocking set in $\mathrm{PG}(2, q)$, containing all lines through Q.

Only when the compromised subscribers form a trivial dual blocking set in $\mathrm{PG}(2, q)$, the TV–net has to distribute a new set of keys to all of their subscribers.

7 Other applications and open problems

In this section, we shall give a brief overview on other applications of blocking sets. The first to mention is on the theory of *t–covers*.

7.1 Covers in Galois geometries

A *t–cover* $\mathcal{C}$ of $\mathrm{PG}(n,q)$ is a set of t–subspaces of $\mathrm{PG}(n,q)$ that cover the point set of $\mathrm{PG}(n,q)$, i.e. every point of $\mathrm{PG}(n,q)$ is contained in at least one element of $\mathcal{C}$. Obviously, $|\mathcal{C}| \geq \lceil \frac{\theta_n}{\theta_t} \rceil$ (we remind that a t–spread, which is a particular case of a t–cover, has size $\frac{\theta_n}{\theta_t}$) and we call the *excess* of $\mathcal{C}$ the integer $\epsilon = |\mathcal{C}| - \lceil \frac{\theta_n}{\theta_t} \rceil$. The *multiple points* of $\mathcal{C}$ are the points contained in more than one element of $\mathcal{C}$ and if P is a multiple point, then the *surplus* of P is the number of elements of $\mathcal{C}$ containing P minus one. One can consider the surplus as a weight function mapping a point $P \in \mathrm{PG}(n,q)$ to a non–negative integer $surplus(P)$. So we have $surplus(P) > 0$ if and only if P is a multiple point and, if $t+1$ divides $n+1$, then $\sum_{P \in PG(n,q)} s!urplus(P) = \epsilon\theta_t$. The following theorem shows the link between blocking sets, more precisely minihypers, and the multiple points of a t–cover.

Theorem 34. *[30] Let $\mathcal{C}$ be a t–cover of $PG(n,q)$, $(t+1)|(n+1)$, with excess $\epsilon < q$. Let F be the set of multiple points of $\mathcal{C}$ and let $w(P) = surplus(P)$, $\forall P \in PG(n,q)$. Then (F,w) is an $(\epsilon\theta_t, \epsilon\theta_{t-1}; n, q)$–minihyper.*

By a classification result about minihypers of [30], it is possible to describe the set of multiple points:

Corollary 3. *[30] Let $\mathcal{C}$ be a t–cover of $PG(n,q)$, $(t+1)|(n+1)$, with excess $\epsilon < \epsilon_q$ where ϵ_q is such that $q+\epsilon_q$ is the size of the smallest non–trivial blocking sets of $PG(2,q)$. Then the multiple points form a sum of ϵ t–subspaces.*

7.2 Minihypers and i–tight sets

By a *polar space*, we will mean the lattice of subspaces of a projective space contained in a non–singular quadric or Hermitian variety, or the lattice of subspaces totally isotropic with respect to a symplectic polarity (see for example [41]). A subset $\mathcal{T}$ of a polar space of rank $r \geq 2$ over $\mathbb{F}_q$ is *i–tight* if

$$|P^\perp \cap \mathcal{T}| = \begin{cases} i\frac{q^{r-1}-1}{q-1} + q^{r-1} & \text{if } P \in \mathcal{T}, \\ i\frac{q^{r-1}-1}{q-1} & \text{if } P \notin \mathcal{T}. \end{cases}$$

The easiest example of an i–tight set of a polar space is the union of i pairwise disjoint generators.

In [19], it has been shown that an i–tight set $\mathcal{T}$ of $W(2r+1,q)$, $Q^+(2r+1,q)$, or $H(2r+1,q)$ is a set of $i\theta_r$ points intersecting every hyperplane in at least $i\theta_{r-1}$ points, hence $\mathcal{T}$ is an $(i\theta_r, i\theta_{r-1}; 2r+1, q)$–minihyper. Using characterization results about minihypers of [19] and [29], it is possible to characterize i–tight sets in the aforementioned polar spaces.

Theorem 35. *[19] An i–tight set on $Q^+(2r+1,q)$, with $2 < i < q/2 - 1$, can only exist for r odd; then such an i–tight set is the union of i pairwise disjoint generators of $Q^+(2r+1,q)$. For every $r \geq 1$, a 1– or 2–tight set on $Q^+(2r+1,q)$ consists of one or two disjoint generators.*

Theorem 36. *[19] Let $\mathcal{T}$ be an i–tight set of $H(2r+1,q)$, with $q > 16$ and $i < q^{\frac{5}{8}}/\sqrt{2}+1$, then $\mathcal{T}$ is the union of pairwise disjoint generators and Baer subgeometries $PG(2r+1,\sqrt{q})$, such that the Hermitian polarity induces a symplectic polarity on these Baer subgeometries.*

Theorem 37. *[19] Let $\mathcal{T}$ be an i–tight set of $W(2r+1,q)$, with q square and $i < q^{\frac{5}{8}}/\sqrt{2}+1$, then $\mathcal{T}$ is the union of pairwise disjoint r–dimensional subspaces and Baer subgeometries $PG(2r+1,\sqrt{q})$. The r–dimensional subspaces are either generators or pairs $\{U, U^\perp\}$, with $U \cap U^\perp = \emptyset$; the subgeometries are either Baer subgeometries invariant under the symplectic polarity or pairs of Baer subgeometries $\{\mathcal{B}_1, \mathcal{B}_2\}$, where $P^\perp \cap \mathcal{B}_2 = PG(2r, \sqrt{q}), \forall P \in \mathcal{B}_1$.*

Since an i–tight set $\mathcal{T}$ of $W(2r+1,q)$, $Q^+(2r+1,q)$, or $H(2r+1,q)$ is an $(i\theta_r, i\theta_{r-1}; 2r+1, q)$–minihyper, improved results on $(i\theta_r, i\theta_{r-1}; 2r+1, q)$–minihypers will imply improved results on these i–tight sets $\mathcal{T}$. As minihypers are blocking sets, we can again state that improved results on blocking sets imply improved results on another topic, i.e. that of i–tight sets of polar spaces.

7.3 t–Fold k–blocking sets in $\mathrm{PG}(n,q)$

Recently, results on 1–fold blocking sets have been extended to t–fold blocking sets. This includes in particular the $1 \pmod{p}$ result (Theorem 10), which was extended to a $t \pmod{p}$ result. Since such $t \pmod{p}$ results are very strong results, implying strong characterization results, we mention this $t \pmod{p}$ result on t–fold blocking sets, and give also a characterization result on t–fold blocking sets heavily relying on this $t \pmod{p}$ result.

Theorem 38. *[26] Let B be a minimal weighted t–fold k–blocking set of $\mathrm{PG}(n,q)$, $q = p^h$, p prime, $h \geq 1$, of size $|B| = tq^k + t + k'$, with $t + k' \leq (q^k - 1)/2$.*

Then B intersects every $(n-k)$–dimensional subspace in $t \pmod{p}$ points.

Theorem 39. *[26] Let B be a minimal weighted t–fold k–blocking set of $\mathrm{PG}(n,q)$, $q = p^h$, p prime, $h \geq 1$, of size $|B| = tq^k + t + k'$, with $t + k' \leq (q^k - 1)/2$.*

Let $e \geq 1$ be the largest integer such that each $(n-k)$–dimensional subspace intersects B in $t \pmod{p^e}$ points. Then, for $0 \leq s \leq n-k$ and every s–dimensional subspace Π_s, $|B \cap \Pi_s| \in \{0, 1, ..., t\} \pmod{p^e}$.

Theorem 40. *[27] Let B be a minimal t–fold k–blocking set in $\mathrm{PG}(n,q)$, q square, $q \geq 661$, $t < c_p q^{1/6}/2$, of size at most $|B| \leq tq^k + 2tq^{k-1}\sqrt{q} < tq^k + c_p q^{k-1/3}$, with $c_2 = c_3 = 2^{-\frac{1}{3}}$ and $c_p = 1$ for $p > 3$.*

Then B is a union of t pairwise disjoint cones $\langle \pi_{m_i}, \mathrm{PG}(2(k-m_i-1), \sqrt{q})\rangle$, $-1 \leq m_i \leq k-1$, $i = 1, \ldots, t$.

Theorem 41. *[27] Let B be a minimal t–fold k–blocking set in $\mathrm{PG}(n,q)$, q square, $t \geq 2$, which is a union of t pairwise disjoint cones $\langle \pi_{m_i}, \mathrm{PG}(2(k-m_i-1), \sqrt{q})\rangle$, $\max\{-1, 2k-n-1\} \leq m_i \leq k-1$. Then $k < n/2$ if B contains at least one k–dimensional space $\mathrm{PG}(k,q)$ and $k \leq n/2$ in the other cases.*

7.4 Blocking sets and semifields

A finite *semifield* $\mathbb{S}$ is a finite algebraic structure satisfying all the axioms of a skew field except (possibly) associativity. These algebraic structures are of considerable interest because they coordinatize certain *translation planes*, called *semifield planes* and two semifields are *isotopic* if and only if the corresponding translation planes are isomorphic. A semifield coordinatizing a Desarguesian plane is isotopic to a field. A geometric construction to get a translation plane is the following: let $\mathcal{S}$ be a $(t-1)$–spread of $\mathrm{PG}(2t-1,q)$, embed $\mathrm{PG}(2t-1,q)$ as a hyperplane into $\mathrm{PG}(2t,q)$, and let $A(\mathcal{S})$ be a point–line geometry such that the points are the points of $\mathrm{PG}(2t,q)\backslash\mathrm{PG}(2t-1,q)$ and the lines are the t–dimensional subspaces of $\mathrm{PG}(2t,q)$ intersecting $\mathrm{PG}(2t-1,q)$ in an element of $\mathcal{S}$ and the incidence is the containment. Then $A(\mathcal{S})$ is a translation plane of order q^t (see e.g. [24]). A spread $\mathcal{S}$ is called a *semifield spread* if $A(\mathcal{S})$ is coordinatized by a semifield. For $\mathrm{PG}(2t-1,q)$, it is always possible to choose as homogeneous coordinates $(x_1,\ldots,x_t;y_1,\ldots,y_t)=(\mathbf{x};\mathbf{y})$ in such a way that the space A of equation $\mathbf{x}=\mathbf{0}$, B of equation $\mathbf{y}=\mathbf{0}$ and C of equation $\mathbf{x}=\mathbf{y}$ are elements of the spread $\mathcal{S}$. Then for every element D of $\mathcal{S}$ distinct from A, there is a unique $t\times t$ matrix J_D over $\mathbb{F}_q$ such that the point $(\mathbf{a};\mathbf{b})$ belongs to D if and only if $\mathbf{b}=\mathbf{a}J_D$. The set $\mathbb{C}=\{J_D|D\in\mathcal{S},D\neq A\}$ is called the *spread set* associated to $\mathcal{S}$ with respect to A,B and C. The spread $\mathcal{S}$ is a semifield spread (with respect to A) if and only if $\mathbb{C}$ is closed under the sum (for more details, see [24, Section 5.1]). Since $\mathbb{C}$ is closed under the sum, there exists a subfield $\mathbb{F}_s$ of $\mathbb{F}_q$ such that $\mathbb{C}$ is a vector space of rank tn over $\mathbb{F}_s$, where $q=s^n$. Embed $\mathrm{PG}(2t-1,q)$ as a canonical subgeometry into $\mathrm{PG}(2t-1,q^t)$ in such a way that $(\mathbf{x};\mathbf{y})\in\mathrm{PG}(2t-1,q)$ if and only if $\mathbf{x}^q=\mathbf{x}$ and $\mathbf{y}^q=\mathbf{y}$, where $\mathbf{x}^q=(x_1^q,\ldots,x_t^q)$. Let A^* and B^* be the spaces of equation $\mathbf{x}=0$ and $\mathbf{y}=0$ respectively. If $P=(\mathbf{b};\mathbf{0})$ is a fixed imaginary point of B^*, then $I=\{(\mathbf{b};\mathbf{b}X)|X\in\mathbb{C}\}$ is the *indicator set* of $\mathcal{S}$ (actually the definition of indicator set appears in a different, more involved way in [52], but here, for the sake of brevity, we give this equivalent way to introduce them) and let $I^*=\{(\lambda\mathbf{b};\mathbf{b}X)|\lambda\in\mathbb{F}_s,X\in\mathbb{C}\}$. Let us now focus on the case $t=2$. Embed $\mathrm{PG}(3,q)$ as a canonical Baer subgeometry into $\mathrm{PG}(3,q^2)$ and let $A^*=\{(x_1,x_2;0,0)|x_i\in\mathbb{F}_{q^2}\}$, then $T=\langle A^*,P\rangle$ is a plane isomorphic to $\mathrm{PG}(2,q^2)$. Then, with the notations as above, we have the following theorem.

Theorem 42. *[52] The spread $\mathcal{S}$ is a semifield spread for $PG(3,q)$ if and only if I^* is a Rédei–type blocking set of $T=PG(2,q^2)$ disjoint from the Baer subline A of A^* which is a Rédei line of I^*.*

The semifields are not only linked to the spreads of projective spaces, but also to *flocks*, and, in [52], it is also shown when a Rédei–type blocking set gives rise to a semifield flock (for the definitions and details, we refer to [52]).

For a survey on the most important results on finite semifields, we refer to the article [47] in the collected work [23].

7.5 Open problems

1) (The linearity conjecture).

All the known examples of small minimal k–blocking sets in $\mathrm{PG}(n,q)$ are linear k–blocking sets. If t such pairwise disjoint small linear k–blocking sets in $\mathrm{PG}(n,q)$ exist, their union is a t–fold k–blocking set in $\mathrm{PG}(n,q)$.

It is generally believed that all small minimal k–blocking sets in $\mathrm{PG}(n,q)$ are linear k–blocking sets, and that all small minimal t–fold k–blocking sets in $\mathrm{PG}(n,q)$ are the union of linear sets, under suitable conditions on the parameters t,k,n,q, and $|B|$. This had led to the following linearity conjecture on blocking sets.

Conjecture 1. (Linearity conjecture for multiple blocking sets [69]) *In $\mathrm{PG}(n,q)$, any t–fold minimal k–blocking set B is the union of some (not necessarily disjoint) linear point sets $B_1,\ldots,B_s$, where B_i is a t_i–fold k–blocking set, and $t_1+\cdots+t_s=t$; provided that t and $|B|$ are small enough ($t \leq T(n,q,k)$ and $|B| \leq S(n,q,k)$ for two suitable functions T and S).*

The proof of this linearity conjecture or parts of this conjecture will imply many new results. As we have mentioned in the preceding sections, improvements to characterization results on blocking sets will open the door to new results on many other problems. That is why we present the problem of proving the linearity conjecture as the central problem on blocking sets.

2) (Maximal partial spreads).

In Theorem 13, a theorem on maximal partial spreads in $\mathrm{PG}(3,q)$, q square, is stated where it is mentioned that the set of holes is the union of s, with $\sqrt{q}-1>s>1$, Baer subgeometries $\mathrm{PG}(3,\sqrt{q})$. Presently, no such examples of maximal partial spreads are known.

Therefore, as a second open problem, we present the problem of proving or disproving the existence of maximal partial spreads in $\mathrm{PG}(3,q)$, q square, satisfying the conditions of Theorem 13.

3) (Extendability of linear codes).

Improvements to the results on the extendability of linear codes are stated in the chapter on Galois geometries and coding theory [46] of [23]. For instance, Maruta proved other extension results [55, 56, 57], including a doubly-extendability result. The conditions that need to be satisfied however are very technical. An open problem is to simplify these conditions. Here, a link with blocking sets or with (weighted) 2–fold blocking sets might occur. In general, is it possible to prove a t–fold extendability result on linear codes involving (weighted) t–fold blocking sets?

References

[1] E.F. Assmus, Jr. and J.D. Key, Designs and their codes, *Cambridge University Press*, 1992.

[2] B. Bagchi and S.P. Inamdar, Projective Geometric Codes, *J. Combin. Theory, Ser. A* **99 (1)** (2002), 128–142.

[3] S. Ball, The number of directions determined by a function over a finite field, *J. Combin. Theory, Ser. A* **104** (2003), 341–350.

[4] B.I. Belov, V.N. Logachev and V.P. Sandimirov, Construction of a class of linear binary codes achieving the Varshamov-Griesmer bound, *Problems of Info. Transmission* **10** (1974), 211–217.

[5] A. Beutelspacher, Blocking sets and partial spreads in finite projective spaces, *Geom. Dedicata* **9 (4)** (1980), 425–449.

[6] A. Blokhuis, Blocking sets in Desarguesian planes. Combinatorics, Paul Erdős is eighty, Vol. 2 (Keszthely, 1993), 133–155, Bolyai Soc. Math. Stud., 2, János Bolyai Math. Soc., Budapest, 1996.

[7] A. Blokhuis, S. Ball, A.E. Brouwer, L. Storme and T. Szőnyi, On the number of slopes of the graph of a function defined on a finite field, *J. Combin. Theory, Ser. A* **86 (1)** (1999), 187–196.

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

[9] A. Blokhuis, P. Sziklai and T. Szőnyi, Blocking sets in projective spaces. Chapter in *Current research topics in Galois geometry* (J. De Beule and L. Storme, Eds.), NOVA Academic Publishers, to appear.

[10] M. Bokler, Minimal blocking sets in projective spaces of square order, *Des. Codes Cryptogr.* **24 (2)** (2001), 131–144.

[11] M. Bokler, Lower bounds for the cardinality of minimal blocking sets in projective spaces, *Discrete Math.* **270 (1–3)** (2003), 13–31.

[12] R.C. Bose and R.C. Burton, A characterization of flat spaces in a finite geometry and the uniqueness of the Hamming and the MacDonald codes, *J. Combin. Theory* **1** (1966), 96–104.

[13] A.A. Bruen, Baer subplanes and blocking sets, *Bull. Amer. Math. Soc.* **76** (1970), 342–344.

[14] A.A. Bruen, Blocking sets in finite projective planes, *SIAM J. Applied Math.* **21** (1971), 380–392.

[15] A.A. Bruen and J.A. Thas, Blocking sets, *Geom. Dedicata* **6 (2)** (1977), 193–203.

[16] A.A. Bruen and J.A. Thas, Hyperplane coverings and blocking sets, *Math. Z.* **81 (3)** (1982), 407–409.

[17] N.J. Calkin, J.D. Key and M.J. de Resmini, Minimum weight and dimension formulas for some geometric codes, *Des. Codes Cryptogr.* **17 (1)** (1999), 105–120.

[18] A. Cossidente, A. Gács, C. Mengyán, A. Siciliano, T. Szőnyi and Zs. Weiner, On large minimal blocking sets in PG$(2,q)$, *J. Combin. Des.* **13 (1)** (2005), 25–41.

[19] J. De Beule, P. Govaerts, A. Hallez and L. Storme, Tight sets, weighted m–covers, weighted m–ovoids and minihypers, *Des. Codes Cryptogr.* **50** (2009), 187–201.

[20] J. De Beule, A. Hallez and L. Storme, A non-existence result on Cameron–Liebler line classes, *J. Combin. Des.* **16 (4)** (2007), 342–349.

[21] J. De Beule, K. Metsch and L. Storme, Characterization results on arbitrary weighted minihypers and on linear codes meeting the Griesmer bound, *Adv. Math. Commun.* **2** (2008), 261–272.

[22] J. De Beule, K. Metsch and L. Storme, Characterization results on arbitrary non-weighted minihypers and on linear codes meeting the Griesmer bound, *Des. Codes Cryptogr.* **49** (2008), 187–197.

[23] J. De Beule and L. Storme (Editors), Current research topics in Galois Geometry, NOVA Academic Publishers, to appear.

[24] P. Dembowski, Finite geometries, *Springer-Verlag, Berlin-New York*, 1968.

[25] S. Ferret and L. Storme, Results on maximal partial spreads in $\mathrm{PG}(3, p^3)$ and on related minihypers, Proceedings of the Conference on Finite Geometries (Oberwolfach, 2001), *Des. Codes Cryptogr.* **29** (2003), no. **1-3**, 105–122.

[26] S. Ferret, L. Storme, P. Sziklai and Zs. Weiner, A $t \pmod p$ result on multiple $(n-k)$–blocking sets in $\mathrm{PG}(n, q)$, *Innov. Incidence Geom.* **6-7** (2007-2008), 169–188.

[27] S. Ferret, L. Storme, P. Sziklai and Zs. Weiner, A characterization of multiple $(n-k)$-blocking sets in projective spaces of square order, *Adv. Geom.*, submitted.

[28] P. Govaerts, Small maximal partial t–spreads, *Bull. Belg. Math. Soc. Simon Stevin* **12 (4)** (2005), 607–615.

[29] P. Govaerts and L. Storme, On a particular class of minihypers and its applications, II: Improvements for q square, *J. Combin. Theory, Ser. A* **97 (2)** (2002), 369–393.

[30] P. Govaerts and L. Storme, On a particular class of minihypers and its applications, I: The result for general q, *Des. Codes Cryptogr.* **28 (1)** (2003), 51–63.

[31] P. Govaerts and L. Storme, The classification of the smallest nontrivial blocking sets in $\mathrm{PG}(n, 2)$, *J. Combin. Theory, Ser. A* **113 (7)** (2006), 1543–1548.

[32] J.H. Griesmer, A bound for error-correcting codes, *IBM J. Res. Develop.* **4** (1960), 532–542.

[33] N. Hamada and T. Helleseth, A characterization of some q-ary codes ($q > (h-1)^2$, $h \geq 3$) meeting the Griesmer bound, *Math. Japonica* **38** (1993), 925–940.

[34] N. Hamada and T. Helleseth, Codes and minihypers. *Optimal codes and related topics.* Proceedings of the EuroWorkshop on Optimal codes and related topics (Sunny Beach, Bulgaria, June 10-16, 2001), pp. 79–84.

[35] N. Hamada and T. Maekawa, A characterization of some q-ary codes ($q > (h-1)^2, h \geq 3$) meeting the Griesmer bound: Part 2, *Math. Japonica* **46** (1997), 241–252.

[36] U. Heim, Blockierende Mengen in endlichen projektiven Raumen, *Mitt. Math. Semin. Giessen* **226** (1996), 4–82.

[37] R. Hill, *A first course in coding theory*, Oxford Applied Mathematics and Computing Science Series (1986).

[38] R. Hill, An extension theorem for linear codes, *Des. Codes Cryptogr.* **17** (1999), 151–157.

[39] R. Hill and P. Lizak, Extensions of linear codes, Proc. Intern. Symposium on Inform. Theory, Canada, 1995, p. 345.

[40] J.W.P. Hirschfeld, Projective Geometries over Finite Fields, *Oxford University Press*, Oxford, 1979.

[41] J.W.P. Hirschfeld and J.A. Thas, General Galois Geometries, *Oxford University Press*, Oxford, 1991.

[42] S. Innamorati and A. Maturo, On irreducible blocking sets in projective planes, *Ratio Math.* **2** (1991), 151–155.

[43] S. Innamorati and A. Maturo, The spectrum of minimal blocking sets, *Discrete Math.* **208/209** (1999), 339–347.

[44] V. Korjik, M. Ivkov, Y. Merinovich, A. Barg and H.C.A. van Tilborg, A broadcast key distribution scheme based on block designs. Cryptography and coding, Lecture Notes of Comput. Sci. (Ed., C. Boyd) 1025, Springer (1995), pp. 3–12.

[45] I. Landjev and A. Rousseva, An extension theorem for arcs and linear codes, *Problems of Info. Transmission* **42**(4) (2006), 65–76.

[46] I. Landjev and L. Storme, Galois geometries and coding theory. Chapter in *Current research topics in Galois geometry* (J. De Beule and L. Storme, Eds.), NOVA Academic Publishers, to appear.

[47] M. Lavrauw and O. Polverino, Finite semifields. Chapter in *Current research topics in Galois geometry* (J. De Beule and L. Storme, Eds.), NOVA Academic Publishers, to appear.

[48] M. Lavrauw, L. Storme, and G. Van de Voorde, On the code generated by the incidence matrix of points and hyperplanes in PG(n, q) and its dual, *Des. Codes Cryptogr.* **48 (3)** (2008), 231–245.

[49] M. Lavrauw, L. Storme, and G. Van de Voorde, On the code generated by the incidence matrix of points and k-spaces in PG(n, q) and its dual, *Finite Fields Appl.* **14 (4)** (2008), 1020–1038.

[50] M. Lavrauw, L. Storme, and G. Van de Voorde, A proof of the linearity conjecture for k-blocking sets in PG(n, p^3), p prime, *J. Combin. Theory, Ser. A*, submitted.

[51] M. Lavrauw, L. Storme, P. Sziklai, and G. Van de Voorde, An empty interval in the spectrum of small weight codewords in the code from points and k-spaces of $\mathrm{PG}(n, q)$, *J. Combin. Theory, Ser. A* **116 (4)** (2009), 996–1001.

[52] G. Lunardon, Blocking sets and semifields, *J. Combin. Theory, Ser. A* **113** (2006), 1172–1188.

[53] G. Lunardon, P. Polito and O. Polverino, A geometric characterisation of linear k-blocking sets, *J. Geom.* **74 (1–2)** (2002), 120–122.

[54] G. Lunardon and O. Polverino, Translation ovoids of orthogonal polar spaces, *Forum Math.* **16 (5)** (2004), 663–669.

[55] T. Maruta, On the extendability of linear codes, *Finite Fields Appl.* **7** (2001), 350–354.

[56] T. Maruta, Extendability of linear codes with minimum distance d, $\gcd(d, q) = 1$, *Discrete Math.* **266** (2003), 377–385.

[57] T. Maruta, A new extension theorem for linear codes, *Finite Fields Appl.* **10** (2004), 674–685.

[58] F.J. MacWilliams and N.J.A. Sloane, The theory of error-correcting codes, *North-Holland Mathematical Library*, Amsterdam-New York-Oxford (1977).

[59] K. Metsch and L. Storme, Partial t-spreads in $\mathrm{PG}(2t + 1, q)$, *Des. Codes Cryptogr.* **18 (1–3)** (1999), 199–216.

[60] P. Polito and O. Polverino, On small blocking sets, *Combinatorica* **18 (1)** (1998), 133–137.

[61] O. Polverino, Small blocking sets in $\mathrm{PG}(2, p^3)$, *Des. Codes Cryptogr.* **20 (3)** (2000), 319–324.

[62] O. Polverino, Linear sets in finite projective spaces, *Discrete Math.* (2009), doi:10.1016/j.disc.2009.04.007.

[63] O. Polverino and L. Storme, Small minimal blocking sets in $\mathrm{PG}(2, q^3)$, *European J. Combin.* **23 (1)** (2002), 83–92.

[64] G. Solomon and J.J. Stiffler, Algebraically punctured cyclic codes, *Inform. and Control* **8** (1965), 170–179.

[65] L. Storme, Linear codes meeting the Griesmer bound, minihypers, and geometric applications, *Le Matematiche* **LIX** (2004), 367–392.

[66] L. Storme, Linear codes meeting the Griesmer bound. Proceedings of the Contact Forum *Coding Theory and Cryptography*, October 7, 2005, at The Royal Flemish Academy of Belgium for Science and the Arts, Brussels, Belgium, (2006), 85–112.

[67] L. Storme and P. Sziklai, Linear pointsets and Rédei type k–blocking sets in $\mathrm{PG}(n, q)$, *J. Algebraic Combin.* **14 (3)** (2001), 221–228.

[68] L. Storme and Zs. Weiner, On 1-blocking sets in PG(n, q), $n \geq 3$, *Des. Codes Cryptogr.* **21 (1–3)** (2000), 235–251.

[69] P. Sziklai, On small blocking sets and their linearity, *J. Combin. Theory, Ser. A* **115 (7)** (2008), 1167–1182.

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

[71] T. Szőnyi, A. Gács and Zs. Weiner, On the spectrum of minimal blocking sets in PG$(2, q)$, Combinatorics, 2002 (Maratea), *J. Geom.* **76 (no. 1-2)** (2003), 256–281.

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

[73] G. Van de Voorde, Blocking Sets in Finite Projective Spaces and Coding Theory, PhD Thesis, 2010.

[74] Zs. Weiner, Small point sets of PG(n, q) intersecting every k-space in 1 modulo $\sqrt{q}$ points, *Innov. Incidence Geom.* **1** (2005), 171–180.

V. Pepe and L. Storme, Department of Mathematics, Ghent University, Krijgslaan 281-S22, 9000 Ghent, Belgium. (valepepe@cage.ugent.be, ls@cage.ugent.be)