Eötvös Loránd University,
Institute of Mathematics

Theses of the PhD dissertation titled

BLOCKING SETS IN FINITE PROJECTIVE SPACES

by Nóra Viola Maloschikné Harrach

Supervisor:
Tamás Szőnyi
Professor, DSc

PhD School of Mathematics
School Leader: Miklós Laczkovich
Professor, Member of the Hungarian Academy of Sciences

Theoretical Mathematics Programme
Head of the programme: András Szűcs
Professor, Corresp. Member of the Hungarian Academy of Sciences

Department of Computer Science,
Faculty of Science, Eötvös Loránd University,
Budapest, Hungary

2013

Introduction

The thesis presents results and constructions concerning blocking sets of the finite projective space $\mathrm{PG}(n, q)$. Throughout the thesis we are mostly working in $\mathrm{PG}(n, q)$, the n-dimensional projective space over the Galois field $\mathrm{GF}(q)$, of order q, where $q = p^h$ and p is a prime. θ_n denotes the number of points in $\mathrm{PG}(n, q)$ and $\theta_n = \frac{q^{n+1}-1}{q-1}$.

Definition 1.4.1. A set B of points in $\mathrm{PG}(n, q)$, which intersects each k-dimensional subspace is called an $(n-k)$*-blocking set* or a *blocking set with respect to k-spaces.*

To exclude trivial cases, $0 < k < n$ will always be assumed.

If no proper subset of B is a blocking set, then B is said to be *minimal.* It is well-known that $|B| \geq \theta_{n-k}$, with equality if and only if B is a subspace of dimension $n - k$.

Small point sets of $\mathrm{PG}(n, q^3)$ intersecting each k-space in $1 \bmod q$ points

A $(n-k)$-blocking set B is called *small* if $|B| < \frac{3}{2}(q^{n-k} + 1)$.

Small minimal $(n-k)$-blocking sets are of special interest, since there is hope to classify them. All the known examples of small minimal blocking sets are linear.

If the order of the projective space is q^m, then a point set S is a *linear set* or a $\mathrm{GF}(q)$-linear subset of $\mathrm{PG}(n, q^m)$, if it is a projected $\mathrm{PG}(s, q)$ subgeometry.

Linear blocking sets have the property that every subspace meets them in $1 \bmod p$ points. It turns out, that the same is true for small minimal $(n-k)$-blocking sets.

Result 1.6.2. (Szőnyi [16], Szőnyi and Weiner [17]) Let B be a small minimal $(n-k)$-blocking set in $\mathrm{PG}(n, q)$, $q = p^h$, p prime. Then each subspace of dimension at least k intersects B in $1 \bmod p$ points.

Conjecture 1.6.3. (Sziklai's Linearity Conjecture, [15]) All small minimal $(n-k)$-blocking sets of $\mathrm{PG}(n, q)$ are linear.

Thus, to every small minimal $(n-k)$-blocking set B an integer $e \geq 1$ can be associated, such that e is the largest integer for which it is true that B meets every k-dimensional subspace in 1 mod p^e points. This integer e is called the *exponent* of B. Sziklai proved in [15] that e is a divisor of h, where $q = p^h$.

In [17] it is proved that if $[l_q(n,k,e), u_q(n,k,e)]$ denotes the smallest interval containing the sizes of all the small minimal $(n-k)$-blocking sets of $\mathrm{PG}(n,q)$, $q = p^h$, $2 < p$ prime, with exponent e, then these intervals are disjoint. Furthermore, if $e'|m$ and $e' < e$, then $u_q(n,k,e) < l_q(n,k,e')$. The best bounds for $l_q(n,k,e)$ and $u_q(n,k,e)$ are due to Blokhuis [7], Polverino [12] and Szőnyi and Weiner [17]. The next statement summarizes some corollaries of the 1 mod p result.

Result 1.6.7. (Szőnyi and Weiner [17]) Assume that B is a point set in $\mathrm{PG}(n,q)$, $q = p^h$, $2 < p$ prime. Let e and k be integers, so that $0 < k < n$ and suppose that $|B| < 3(q^{n-k}+1)/2$. Then the following statements are equivalent:

(1) B is a minimal $(n-k)$-blocking set and $|B| \leq u_q(n,k,e)$.

(2) B intersects each k-space in 1 mod p^e points.

(3) Every subspace with dimension at least k intersects B; and any subspace that intersects B intersects it in 1 mod p^e points.

Starting from the smallest one, the first interval consists of one value only, $l_q(n,k,h) = u_q(n,k,h) = \theta_{n-k}$, because an $(n-k)$-dimensional subspace is the only $(n-k)$-blocking set with the property that every subspace of dimension at least k intersects it in 1 mod q points.

When q is a square (hence $2|h$), then $[l_q(n,k,h/2), u_q(n,k,h/2)]$ is the second interval. Weiner proves in [18] that if $q = p^h$, $2 < p$ prime, $81 \leq q$, then small minimal blocking sets of $\mathrm{PG}(n,q)$, with size belonging to the interval $[l_q(n,k,h/2), u_q(n,k,h/2)]$, are linear. In other words, small minimal blocking sets meeting every k-space in 1 mod $\sqrt{q}$ points are linear. A corollary of this result is that the Linearity Conjecture is valid in projective spaces $\mathrm{PG}(n,p^2)$, $p > 11$ prime.

The next interval to be observed is $[l_q(n,k,h/3), u_q(n,k,h/3)]$, if h is divisible by 3. The next result solves the planar case. For sake of simplicity we will change the order of the projective space from q to q^3.

Result 1.6.11. (Polverino [12], Polverino and Storme [13]) A non-trivial blocking set in $\mathrm{PG}(2, q^3)$, $q = p^h$, $p \geq 7$ prime, meeting every line in 1 mod q points is either a Baer subplane (and h is even) or a projected $\mathrm{PG}(3, q)$ subgeometry. In this latter case either $|B| = q^3+q^2+1$ or $|B| = q^3+q^2+q+1$.

In a joint work with Zsuzsa Weiner, Klaus Metsch and Tamás Szőnyi we proved the general case. This appeared in [4] (case $k = 1$) and [3] (case $k \geq 2$).

Theorem 2.1.1. ([3],[4]) Let B be a point set of $\mathrm{PG}(n, q^3)$, $q = p^h$, $1 \leq h$, $7 \leq p$ prime, intersecting each k-space in 1 mod q points, and with size $|B| < \frac{3}{2}(q^{3(n-k)} + 1)$. Then B is a linear $(n-k)$-blocking set.

Corollary 2.1.2. Let s be the smallest integer such that $3 < s \leq 3h$ and $s|3h$. Then all the minimal $(n-k)$-blocking sets of size $< l_{q^3}(n, k, 3h/s)$ are linear.

Another important corollary of Theorem 2.1.1 is that it proves the Linearity Conjecture in projective spaces of order p^3, with $p \geq 7$ prime.

Corollary 2.1.3. Small minimal blocking sets of $\mathrm{PG}(n, p^3)$, $p \geq 7$ prime are linear.

The following technique was used to prove Theorem 2.1.1 for $k = 1$: combinatorial and geometric arguments prove that every line meets the set in a linear point set, and that many of the plane sections of the set are also linear. Then, with algebraic methods a linear subset is 'built' in B. To solve the case $k \geq 2$, similar reasonings could be used, but in the thesis we present a slightly different technique. We project our set B to a hyperplane of the projective space and prove that the resulting set B' is a blocking set with respect to $(k-1)$-spaces of the hyperplane. By induction on k, we can assume that B' is linear and then 'lift the linear structure' to the set B.

Both methods have the advantage that one needs to study only the plane sections of the blocking set. There is hope that these techniques may be generalized in order to help solving similar problems. For example in the classification of small blocking sets in $\mathrm{PG}(n, q^h)$ for $h > 3$, or even in the classification of sets of points in $\mathrm{PG}(n, q^h)$ that meet every plane in a linear set.

In [3] we give a classification of projected $\mathrm{PG}(6, q)$ subgeometries of $\mathrm{PG}(3, q^3)$. By Theorem 2.1.1, these are the minimal 2-blocking sets with size in the interval $[l_{q^3}(n, n-2, h), u_{q^3}(n, n-2, h)]$. There are four types of such sets: two are cones over planar blocking sets, one is a Rédei type blocking set and the last one is not of Rédei type.

Unique reducibility of multiple blocking sets

Definition 1.7.1. A *t-fold* $(n-k)$*-blocking set* of $\mathrm{PG}(n, q)$ is a set of points which meets every k-dimensional subspace in at least t points. If the points of the set are not all different, so the set is a *multiset* of points, then it is called a *weighted* t-fold $(n-k)$-blocking set.

To exclude trivial cases, $0 < k < n$ will always be assumed.

A weighted t-fold $(n-k)$-blocking set is said to be *minimal* if no proper subset of it is a (weighted) t-fold $(n-k)$-blocking set. If a weighted t-fold $(n-k)$-blocking set is not minimal, then it contains a minimal weighted t-fold $(n-k)$-blocking set: we can examine the points one by one, and remove "unnecessary" points. But it may happen, that if we examine the points in a different order, then the minimal weighted t-fold $(n-k)$-blocking set we arrive at is different. The next theorem is proved in [1].

Theorem 3.1.3. ([1]) A weighted t-fold $(n-k)$-blocking set of $\mathrm{PG}(n, q)$, with total weight smaller than $(t+1)q^{n-k} + \theta_{n-k-1}$ contains a unique minimal weighted t-fold $(n-k)$-blocking set.

Our result is a generalization of a result proved by Szőnyi for $n = 2$, $t = 1$ in [16], and a similar (slightly weaker) result presented by Lavrauw, Storme and Van de Voorde for $n \geq 2$, $t = 1$ in [11].

For the proof of Theorem 3.1.3 we prove a lemma on t-fold nuclei of weighted sets (Lemma 3.3.4), which is a generalization of similar results by Sziklai in [14] and Ball in [6].

A line ℓ is called a t-secant of the weighted set B, if the weight of ℓ is exactly t.

Corollary 3.5.9. Let B be a (weighted) t-fold $(n-1)$-blocking set of $\mathrm{PG}(n,q)$, and $P \in B$. Then there are at least $(t+1)q^{n-1}+\theta_{n-2}-|B|$ t-secants through P.

This corollary is in fact equivalent to Theorem 3.1.3, if $k=1$. For $n=2$, similar results have been proved by Ferret, Storme, Sziklai and Weiner in [9] and Bacsó, Héger and Szőnyi in [5]. A somewhat better result for non-weighted sets has been proved by Blokhuis, Lovász, Storme and Szőnyi in [8]. The next example shows that Theorem 3.1.3. is sharp if $t=1$.

Example 3.5.1. Let Σ^1 and Σ^2 be two $(n-k)$-dimensional subspaces of $\mathrm{PG}(n,q)$ meeting in an $(n-k-1)$-dimensional subspace. Then $B := \Sigma^1 \cup \Sigma^2$ contains two different minimal 1-fold $(n-k)$-blocking sets, Σ^1 and Σ^2, and $|B| = 2q^{n-k}+\theta_{n-k-1}$.

For $t \geq q+1$ the proof of Theorem 3.1.3 yields that it cannot be sharp. The following example shows the sharpness, when $2 \leq t \leq q$.

Example 3.5.6. Let π be a plane of $\mathrm{PG}(n,q)$, let $l_1, l_2, \ldots, l_t$ be different lines in π through a common point P, and l_{t+1} a further line of π, with $P \notin l_{t+1}$. Then the multiset $B := (l_1+l_2+\cdots+l_t) \cup l_{t+1}$ is a t-fold $(n-1)$-blocking set in $\mathrm{PG}(n,q)$, $|B| = t(q+1)+(q+1-t) = (t+1)q+1$, and $l_1+l_2+\cdots+l_t$ and $l_1 \cup (l_2+\cdots+l_t) \cup l_{t+1}$ are two minimal t-fold $(n-1)$-blocking sets contained in B; the latter one differs from B only in the point P.

Construction 3.5.10. (1) Let B be a minimal t-fold $(n-1)$-blocking set, which has a point $P \in B$, through which there are exactly $(t+1)q^{n-1}+\theta_{n-2}-|B|$ t-secants to B. Adding a point to every t-secant will result in a t-fold $(n-1)$-blocking set S of size $(t+1)q^{n-1}+\theta_{n-2}$ and containing two different minimal t-fold $(n-1)$-blocking sets.

(2) Embed the set S in an $(n-k+1)$-dimensional subspace of $\mathrm{PG}(n,q)$ to obtain t-fold $(n-k)$-blocking sets of size $(t+1)q^{n-k}+\theta_{n-k-1}$, which contain two different minimal t-fold $(n-k)$-blocking sets.

For $n=2$, $k=1$ and $1 \leq t \leq q$ one can find t-fold 1-blocking sets in $\mathrm{PG}(2,q)$ which have points that are on exactly $(t+1)q+1-|B|$ t-secants to B. The sum of t Rédei type blocking sets which have a common Rédei line, and share exactly one point, which is not on the Rédei line will have this property. Using such a planar t-fold 1-blocking set and Construction 3.5.10(2), we get examples for $n \geq 3$, $k = n - 1$ and $1 \leq t \leq q$. Example 3.5.6 is a special case of this: the sum of t lines sharing a common point.

Unfortunately, for $t \geq 2$, $n \geq 3$ and $k = 1$, in the minimal t-fold $(n-1)$-blocking sets we examined, all points have at least $t\theta_{n-1} - (q+1-t)q^{n-2} - |B|$ t-secants to B. Thus, it may be conjectured that the correct bound in Theorem 3.1.3 should be

$$t\theta_{n-k} + (q + 1 - t)q^{n-k-1}.$$

A generalization of the Megyesi construction

Consider the projective plane $\mathrm{PG}(2, q)$ as the union $\mathrm{AG}(2, q) \cup \ell_\infty$.

Definition 1.5.1. We say that *the ideal point* $Q \in \ell_\infty$ *is determined* by the affine points $P_1, P_2 \in \mathrm{AG}(2, q)$, if the line $\langle P_1, P_2\rangle$ meets ℓ_∞ in Q.

In Rédei's blocking set construction a set U of q points is selected in $\mathrm{AG}(2, q)$, and U together with $D \subset \ell_\infty$, the set of ideal points determined by U, form a minimal blocking set if $|D| < q + 1$. The Megyesi construction is a special case of this.

Megyesi construction. Let G be a multiplicative subgroup of $\mathrm{GF}(q)^* := \mathrm{GF}(q) \setminus \{0\}$, and $U = \{(a, 0) : a \in G\} \cup \{(0, b) : b \notin G\} \cup \{(0, 0)\}$. We say that G was *'placed'* on the line $y = 0$ and the complementer of G was 'placed' on the line $x = 0$. If D denotes the set of ideal points determined by U, then $D = \{(0), (\infty)\} \cup \{(m) : m \notin G\}$, and with $B := U \cup D$, the resulting minimal blocking set has size $|B| = 2q + 1 - |G|$.

In [10] Gács gave a similar construction, choosing a multiplicative subgroup of index three and 'placing' the cosets of this subgroup on three concurrent lines. The resulting minimal blocking sets have size approximately $2q - \frac{2}{9}q$. In a joint work with Csaba Mengyán we generalized this construction, by placing the cosets of a multiplicative subgroup of order s of $\mathrm{GF}(q)^*$ on n concurrent lines ($n \leq s$). Our results appeared in [2]. For sake of simplicity here we only present the case when $n = 3$, so the cosets are placed on three lines.

Construction 4.1.1. Let $s \geq 3$ be a divisor of $q-1$ and consider a multiplicative subgroup G of $\mathrm{GF}(q)^*$ with index s. Let $\alpha \in \mathrm{GF}(q)^*$ be an element for which G, αG, $\alpha^2 G$, ..., $\alpha^{s-1}G$ are the cosets of G. Form three non-empty subsets $I, J, K \subset \mathbb{Z}_s$ such that $|I|+|J|+|K| = s$. Let

$$U = \{(0,x) : x \in \alpha^i G, i \in I\} \cup \{(x,0) : x \in \alpha^j G, j \in J\} \cup \\ \cup \{(x,x) : x \in \alpha^k G, k \in K\} \cup \{(0,0)\}.$$

Denote by D the set of directions determined by U. If $|D| < q+1$, then $B = U \cup D$ is a minimal blocking set.

The size of the minimal blocking set B of Construction 4.1.1. can be determined by determining $|D|$. It is more convenient for us to determine $D^c := \ell_\infty \setminus D$, and clearly $|D| + |D^c| = q+1$.

Notation. Let I, J, K be non-empty subsets of $\mathbb{Z}_s$, such that $|I|+|J|+|K| = s$. Denote by $T(I,J,K)$ the set of ordered pairs $(u,v) \in \mathbb{Z}_s \times \mathbb{Z}_s$, for which I, $J+u$ and $K+v$ are pairwise disjoint (that is $\mathbb{Z}_s$ is a disjoint union of I, $J+u$ and $K+v$).

Basic calculations prove that $|T(I,J,K)| \leq 2s^2/9$ (Proposition 4.1.7).

Theorem 4.1.6. Let D^c be the set of non-determined directions in Construction 4.1.1. Then

$$|D^c| = \frac{|T(I,J,K)|}{s^2} q + C\sqrt{q} \leq \frac{2}{9} q + C\sqrt{q},$$

with $|C| \leq 4s^2/9$. If $s = o(\sqrt[4]{q})$, then

$$|B| \geq \left(2 - \frac{2}{9}\right) q + O(\sqrt{q}s^2).$$

To prove Theorem 4.1.6 a variant of the Weil estimate is used. In the following theorem we find some values which can be achieved.

Theorem 4.1.12. Let s be a divisor of $q-1$, $s \geq 3$. In $\mathrm{PG}(2,q)$ minimal blocking sets of sizes $2q - \frac{q}{s^2} + C_1\sqrt{q}$, and $2q - \frac{2q}{s^2} + C_2\sqrt{q}$ exist, with $|C_i| \leq 2i$ If k and l are divisors of s, such that $kl < s$, then minimal blocking sets of size $2q - \frac{kl}{s^2} q + C_{kl}\sqrt{q}$ exist, with $|C_{kl}| \leq 2kl$.

The last section of [2] presents constructions of blocking sets in $\mathrm{PG}(2, q^h)$, $h > 1$, from blocking sets of $\mathrm{PG}(2, q)$. We start with a minimal blocking set B of $\mathrm{PG}(2, q)$, we embed $\mathrm{PG}(2, q)$ into $\mathrm{PG}(2, q^h)$ as a subgeometry, and then we add some points of $\mathrm{PG}(2, q^h) \setminus \mathrm{PG}(2, q)$ to B to make it a minimal blocking set in $\mathrm{PG}(2, q^h)$. If $|B| = 2q - x$, with $x \geq 1$, then the resulting blocking sets have size $2q^h - x$ and $2q^h - x + 1$. If B is a Rédei type minimal blocking set, then with a careful choice of the construction it can be achieved that the resulting set is also of Rédei type.

This thesis is based on

HaUnique [1] N. V. Harrach. Unique reducibility of multiple blocking sets. *J. Geom.*, 103:445–456, 2012.

HaMen [2] N. V. Harrach and C. Mengyán. Minimal blocking sets in $\mathrm{PG}(2, q)$ arising from a generalized construction of megyesi. *Innov. Incidence Geom.*, 6/7:211–226, 2007/2008.

HaMe [3] N. V. Harrach and K. Metsch. Small point sets of $\mathrm{PG}(n, q^3)$ intersecting each k-subspace in 1 mod q points. *Designs, Codes and Cryptography*, 56(2-3):235–248, 2010.

HaMeSzoWe [4] N. V. Harrach, K. Metsch, T. Szőnyi, and Zs. Weiner. Small point sets of $\mathrm{PG}(n, p^{3h})$ intersecting each line in 1 mod p^h points. *Journal of Geometry*, 98(1-2):59–78, 2010.

Further references

BaHeSzo [5] G. Bacsó, T. Héger, and T. Szőnyi. The 2-blocking number and the upper chromatic number of $\mathrm{PG}(2, q)$. *J. Comb. Des.*, 21:585–602, 2013.

Ball [6] S. Ball. On nuclei and blocking sets in Desarguesian spaces. *J. Combin. Theory Ser. A*, 85:232–236, 1999.

Blokhuis4 [7] A. Blokhuis. Blocking sets in desarguesian planes. *Bolyai Soc. Math. Studies*, 2:133–155, 1996. Paul Erdős is Eighty.

BloLoStoSzo [8] A. Blokhuis, L. Lovász, L. Storme, and T. Szőnyi. On multiple blocking sets in Galois planes. *Adv. Geom.*, 7:39–53, 2007.

FeStoSziWe [9] S. Ferret, L. Storme, P. Sziklai, and Zs. Weiner. A characterization of multiple $(n-k)$-blocking sets in projectiove spaces of square order. *Adv. Geom.*, 14:739–756, 2012.

gacs [10] A. Gács. On the number of directions determined by a point set in $\mathrm{AG}(2,p)$. *Discrete Math.*, 208/209:299–309, 1999.

LaStoVan [11] M. Lavrauw, L. Storme, and G. Van de Voorde. On the code generated by the incidence matrix of points and k-spaces in $\mathrm{PG}(n,q)$ and its dual. *Finite Fields Appl.*, 14:1020–1038, 2008.

Polverino [12] O. Polverino. Small minimal blocking sets and complete k-arcs in $\mathrm{PG}(2,p^3)$. *Discrete Math.*, 208/209:469–476, 1999.

PoSto [13] O. Polverino and L. Storme. Small minimal blocking sets in $\mathrm{PG}(2,q^3)$. *European J. Combin.*, 23(1):83–92, 2002.

Sziklai [14] P. Sziklai. Nuclei of point sets in $\mathrm{PG}(n,q)$. *Discrete Math.*, 174:323–327, 1997.

Sziklai4 [15] P. Sziklai. On small blocking sets and their linearity. *J. Combin. Theory Ser. A*, 115(7):1167–1182, 2008.

Szonyi [16] T. Szőnyi. Blocking sets in Desarguesian affine and projective planes. *Finite Fields Appl.*, 3(3):187–202, 1997.

SzoWe [17] T. Szőnyi and Zs. Weiner. Small blocking sets in higher dimensions. *J. Combin. Theory Ser. A*, 95(1):88–101, 2001.

Weiner [18] Zs. Weiner. Small point sets of $\mathrm{PG}(n,q)$ intersecting each k-space in 1 modulo $\sqrt{q}$ points. *Innov. Incidence Geom.*, 1:171–180, 2005.