

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2024  
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2024  
*Proceedings of the Fifty-Third Spring Conference  
of the Union of Bulgarian Mathematicians  
Borovets, April 1–5, 2024*

ON AFFINE BLOCKING SETS\*

Assia Rousseva

Faculty of Mathematics and Informatics,  
Sofia University “St. Kliment Ohridski”, Sofia, Bulgaria  
e-mail: [assia@fmi.uni-sofia.bg](mailto:assia@fmi.uni-sofia.bg)

We survey the known results on the minimal size of a blocking set in the finite affine geometries  $AG(n, q)$ .

**Keywords:** finite affine geometries, finite projective geometries, arcs, blocking sets, linear codes, Bruen’s bound.

АФИННИ БЛОКИРАЩИ МНОЖЕСТВА

Ася Русева

Факултет по математика и информатика,  
Софийски университет „Св. Климент Охридски“, София, България  
e-mail: [assia@fmi.uni-sofia.bg](mailto:assia@fmi.uni-sofia.bg)

В статията е направен обзор на известните резултати върху задачата за намиране на минималната мощност на блокиращо множество в  $AG(n, q)$ .

**Ключови думи:** крайни афинни геометрии, крайни проективни геометрии, арки, блокиращи множества, линейни кодове, граница на Бруен.

**1. Introduction.** A set of points  $\mathcal{B}$  in an affine geometry  $AG(n, q)$ ,  $q = p^h$ ,  $p$  a prime number, is called a  $t$ -fold blocking set, or a  $t$ -fold intersection set with respect to hyperplanes, if  $|\mathcal{B} \cap H| \geq t$  for every hyperplane  $H$  in  $AG(n, q)$  and there exists a hyperplane  $H_0$  with  $|\mathcal{B} \cap H_0| = t$ . A  $t$ -fold blocking set  $\mathcal{B}$  in  $AG(n, q)$  with  $|\mathcal{B}| = N$  is referred to as an  $(N, t)$ -blocking set. In this paper, we deal with the following problem:

Given a positive integer  $t$  and a prime power  $q = p^h$ , determine the minimal size of a  $t$ -fold blocking set in  $AG(n, q)$ .

---

\* <https://doi.org/10.55630/mem.2024.53.009-017>

This research was supported by the Bulgarian National Science Foundation under Contract KP-06-N72/6-2023.

**2020 Mathematics Subject Classification:** 51E15, 51E21, 51E22, 51A05, 94B05.

The first results on affine blocking sets were obtained independently by Jamison [11] and Brouwer and Schrijver [8]. They proved that for a 1-fold blocking set  $\mathcal{B}$  in  $\text{AG}(n, q)$  one has the lower bound

$$|\mathcal{B}| \geq n(q-1) + 1.$$

This has been generalized by Bruen in a seminal paper [9], and later on by Ball and Blokhuis. Constructions of good affine blocking are scarce and consist mainly in taking a union of lines with carefully chosen directions.

This survey is structured as follows. In Section 2, we give an overview of the known lower bounds on the size of a  $t$ -fold blocking set. Section 3 contains the known constructions for blocking sets meeting Bruen's bound. In section 4, we present a general construction in  $\text{AG}(n, q)$  which gives in many cases optimal blocking sets.

**2. Lower bounds on the size of an affine blocking set.** The first lower bound on the size of an affine blocking set was obtained by Jamison [11].

$$(1) \quad |\mathcal{B}| \geq n(q-1) + 1.$$

The same result was proved by Brouwer and Schrijver in [8]. They pointed out that the bound is sharp for all dimensions  $n$ . In the example below we sketch the proof of the fact that the size of a blocking set in  $\text{AG}(2, q)$  has at least  $2q-1$  points. The Jamison bound for an arbitrary dimension is easily obtained by considering polynomials in  $n$  variables.

**Example 1.** Let  $\mathcal{B}$  be a blocking set in  $\text{AG}(2, q)$ . Without loss of generality one can take  $(0, 0) \in \mathcal{B}$ . By doing this, we block all lines through  $(0, 0)$ . The lines not incident with  $(0, 0)$  have equations  $uX + vY = 1$ . Define:

$$F(X, Y) = \prod_{(b_1, b_2) \in \mathcal{B} \setminus \{(0,0)\}} (b_1X + b_2Y - 1).$$

Clearly,  $F(u, v) = 0$  for all  $(u, v) \in \mathbb{F}_q^2 \setminus \{(0, 0)\}$ . The polynomial  $F$  can be written in the form

$$F(X, Y) = F_1(X, Y)(X^q - X) + F_2(X, Y)(Y^q - Y) + G(X, Y),$$

where the degree of  $G$  in  $X$  and in  $Y$  does not exceed  $q-1$ , i.e.  $\deg_X G \leq q-1$  and  $\deg_Y G \leq q-1$ . Now the polynomials  $XF(X, Y)$  and  $YF(X, Y)$  are zero for all  $(u, v) \in \mathbb{F}_q^2$ . Hence  $XG(X, Y)$  and  $YG(X, Y)$  are also zero for all  $(u, v) \in \mathbb{F}_q^2$ . By the Combinatorial Nullstellensatz [1]

$$XG(X, Y) = G_1(X, Y)(X^q - X) + G_2(X, Y)(Y^q - Y),$$

whence  $G_2 \equiv 0$  and  $X^{q-1} - 1$  divides  $G$ . Similarly,  $Y^{q-1} - 1$  divides  $G$ . Hence

$$|\mathcal{B}| - 1 = \deg F \geq \deg G \geq 2(q-1).$$

A generalization of the Jamison bound to subspaces of arbitrary dimension was given by Bruen in [9].

**Theorem 2** ([9]). *For a  $t$ -fold blocking set  $\mathcal{B}$  with respect to the hyperplanes in  $\text{AG}(n, q)$  one has*

$$(2) \quad |\mathcal{B}| \geq (n+t-1)(q-1) + 1.$$

In what follows we call this bound *the Bruen bound*. The bound is non-trivial for values of  $t$  satisfying  $1 \leq t \leq (n-1)(q-1)$ . For  $t > (n-1)(q-1)$  Bruen's bound becomes worse than the trivial bound

$$|\mathcal{B}| \geq tq,$$

obtained by counting the points of the blocking set on  $q$  parallel hyperplanes.

The proof of (2) is algebraic and does not give an idea how to construct blocking sets that meet this bound. It was pointed out by Zanella [17] that for

$$t > \frac{(n-1)(q-1)+1}{2}$$

blocking sets meeting the Bruen bound do not exist.

In [2] Ball proved that the Bruen bound cannot be attained if the parameters  $t, n$  and  $q$  satisfy some special numerical condition. Using the polynomial method he proved the following theorem.

**Theorem 3** ([2]). *For  $t < q$  a  $t$ -fold blocking set with respect to hyperplanes in  $AG(n, q)$  has at least  $(n+t-1)(q-1)+k$  points provided there exists a  $j$  with  $k-1 \leq j < t$  such that the binomial coefficient  $\binom{k-n-t}{j} \not\equiv 0 \pmod{p}$ .*

For  $k = t$ , i.e.  $j = t - 1$  one gets the following corollary.

**Corollary 4** ([2]). *For  $t < q$  a  $t$ -fold blocking set with respect to hyperplanes in  $AG(n, q)$  has at least  $(n+t-1)q - n + 1$  points provided*

$$\binom{-n}{t-1} \not\equiv 0 \pmod{p}.$$

The next two theorems improve the bounds from Theorems 2 and 3. However the bounds they provide are not explicit. The proofs of these results give no idea about the structure of the blocking sets that meet the corresponding bounds.

**Theorem 5** ([5]). *Let there exist an  $(N, t)$ -blocking set in  $AG(n, q)$ , where  $q = p^h$ , and  $p$  is a prime. Then for all integers  $\varepsilon \geq 1$  the coefficient of  $X^{N-tq+\varepsilon}$  in*

$$(X-1)^{N-q^n} (X^p-1)^{\frac{(q^{n-1}-t)q}{p}}$$

is divisible by  $q^n$ .

**Theorem 6** ([6]). *Assume there exists an  $(N, t)$ -blocking set in  $AG(n, q)$ , where  $q = p^h$ , and  $p$  is a prime, with*

$$N = (t+n+1-e)q - n - 1 - \varepsilon,$$

where  $e \in \{1, \dots, t-1\}$  and  $\varepsilon \geq 1$  is an integer. Then

$$\sum_{j=0}^{n-1} (-1)^j \binom{-t+e-1}{j} \binom{N}{(t-e+1)q - \varepsilon + j(q-1)} \equiv 0 \pmod{p^e}.$$

The proofs of these results are algebraic and use the so-called polynomial method (see also [3, 4, 7]).

**3. Blocking sets meeting Bruen's bound.** Affine blocking sets with  $t = 1$  exist in affine geometries of arbitrary dimension  $n$ . This fact was noted by Brouwer and Schrijver in [8] who proved that a pencil of  $n$  lines in general position is such a blocking set. This blocking set is clearly not unique. One might also construct such blocking sets by induction starting from the affine line  $AG(1, q)$ . Given a blocking set in  $AG(n, q)$  of size  $n(q-1)+1$  construct a new blocking set in  $AG(n+1, q)$  by taking  $n(q-1)+1$  points in any hyperplane  $H$  that form such a blocking set plus  $q-1$  additional points – one in each hyperplane parallel to  $H$ .

It was noted by Ball in [2] and by Zanella in [17] that a  $(q^2, q-1)$ -blocking set in  $AG(3, q)$  can be obtained if we delete a tangent plane from the hyperbolic quadric in

$\text{PG}(3, q)$ . Such blocking set meets obviously the Bruen bound for  $n = 3$  and  $t = q - 1$ .

A non-trivial example of blocking sets with  $t = 2$  lying on the Bruen bound was constructed by Ball in [2].

Fix an  $(n + 1)$ -arc with points  $P_i, i = 1, \dots, n + 1$ , in a hyperplane  $H$  of  $\text{PG}(n + 1, q)$ . Select lines  $L_i$  in  $\text{PG}(n, q)$  with  $P_i \in L_i$  in such a way that  $L_i \cap L_n = Q_{i,i+1}$ ,  $L_{n+1} \cap L_1 = Q_{n+1,1}$ . Let  $\mathcal{B}$  be the union of these lines outside  $H$ . All planes are blocked twice apart from  $H_{i,i+1} = \langle P_1, \dots, P_{i-1}, Q_{i,i+1}, P_{i+2}, P_{n+1} \rangle$  and  $H_{n+1,1} = \langle P_2, \dots, P_n, Q_{n+1,1} \rangle$ . The point  $P \in H_{1,2} \cap H_{2,3} \cap \dots \cap H_{n,n+1}$  is from  $\text{AG}(n, q) = \text{PG}(n, q) \setminus H$ . Now for every  $Q \in H_{n+1,n}$   $\mathcal{B} \cup \{P, Q\}$  is an affine 2-fold blocking set of size  $(n + 1)q - n + 3$ . If one can choose  $P = Q$  then the blocking set has one point less and meets the Bruen bound. By Theorem 3 this should only be possible for  $n \equiv 0 \pmod{p}$ . In [2] Ball shows that this condition is also sufficient. The construction is presented on the figure below.

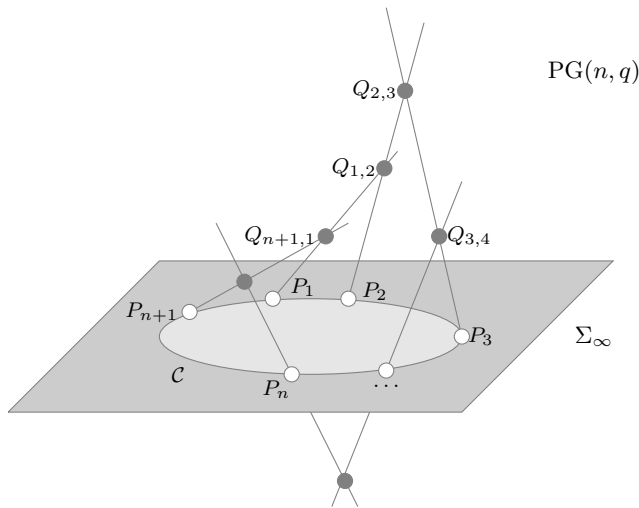


Fig. 1. An  $((n + 1)q - n + \varepsilon, 2)$ -blocking set in  $\text{AG}(n, q)$

It has been pointed out by Ball in [2] that in all cases with  $t + n = q + 2$ , Theorem 3 does not improve on the Bruen bound. In fact, it was demonstrated in [14] that in this case blocking sets meeting the Bruen bound can be constructed.

**Theorem 7** ([14]). *There exists a  $(q^2, q - n + 2)$ -blocking set in  $\text{AG}(n, q)$  for every prime power  $q$  and every  $3 \leq n \leq q - 1$ .*

**Proof.** Let  $T$  be subspace of codimension 2 in  $\Omega \cong \text{PG}(n, q)$  and denote by  $H_0, \dots, H_q$  the hyperplanes through  $T$  in  $\Omega$ . Fix  $q + 1$  points  $x_1, \dots, x_q$  in  $T$  that form a  $(q + 1)$ -arc, a normal rational curve minus a point, say. In each of the hyperplanes  $H_i, i = 1, \dots, q$ , select a line  $L_i$  meeting  $T$  in  $x_i$ . Now the set of points

$$\mathcal{B} = \bigcup_{i=1}^q (L_i \setminus x_i)$$

is a  $(q - n + 2)$ -fold blocking set in  $\Omega \setminus H_0 \cong \text{AG}(n, q)$ . This construction is presented on Figure 2 below.  $\square$

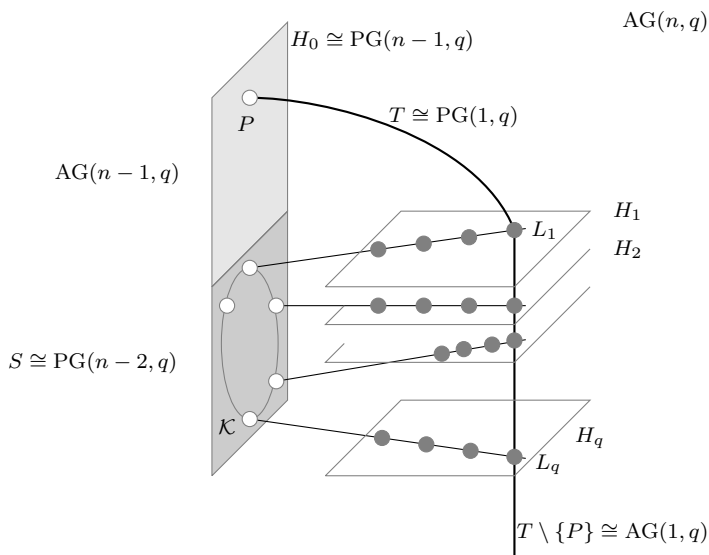


Fig. 2. The  $(q^2, q - n + 2)$ -blocking set in  $AG(n, q)$

This construction can be modified further to construct  $t$ -fold blocking sets of relatively small size that are close to being optimal. They are obtained by removing  $n - 2 + s$  points from each of the lines  $L_1, \dots, L_s$  chosen as in Theorem 7.

**Theorem 8.** *For every  $s = 0, 1, \dots, q+1-n$ , there exist  $(q^2 - s(n-2+s), q - (n-2+s))$ -blocking sets in  $AG(n, q)$ .*

In the case  $s = 1$  we get an optimal blocking set that meets the bound from Theorem 3.

**Corollary 9.** *For every  $q$  there exists an affine blocking set with parameters  $(q^2 - n + 1, q - n + 1)$  in  $AG(n, q)$ . Blocking sets of this size are optimal.*

The optimality of the latter is proved by Corollary 4. Indeed, we have

$$\binom{-n}{t-1} = \frac{(-n) \cdot (-n-1) \dots (-q+1)}{(q-n)!}.$$

Since for  $i = 0, \dots, q - n - 1$ ,  $-n - i$  and  $q - n - i$  are divided by the same power of  $p$ , we get that  $\binom{-n}{t-1} \not\equiv 0 \pmod{p}$ .

Summing up, up to this moment the only known families of blocking sets meeting the Bruen bound are the following:

- (1)  $t = 1$ : for all  $n$  and all  $q$  (Brouwer-Schrijver);
- (2)  $t = 2$ : for all  $n \equiv 0 \pmod{p}$ , where  $p = \text{char } \mathbb{F}_q$  (Ball);
- (3)  $t = q - n + 2$ : for all  $3 \leq n \leq q - 1$  and all  $q$  (Landjev-Rousseva).

It is conjectured that blocking sets meeting the Bruen bound do not exist for  $t \geq q$ .

**4. General constructions.** We start this section with a theorem which describes a general construction for blocking sets in  $\text{AG}(n, q)$ .

**Theorem 10** ([15]). *Let  $n \geq 3$  be a positive integer and let  $q = p^h$  be a prime power. Assume there exist*

- an  $(M, w)$ -arc in  $\text{PG}(r, q)$ , where  $2 \leq r \leq n - 2$ , and
- an  $(M', u)$ -blocking set in  $\text{AG}(n - r - 1, q)$ .

*Then there exists an  $(N, t)$ -blocking set in  $\text{AG}(n, q)$  with*

$$N = qM, \quad t = \min\{M - w, aqu\},$$

*where  $a = \lfloor M/M' \rfloor$ .*

The theorem is presented on Figure 3 below.

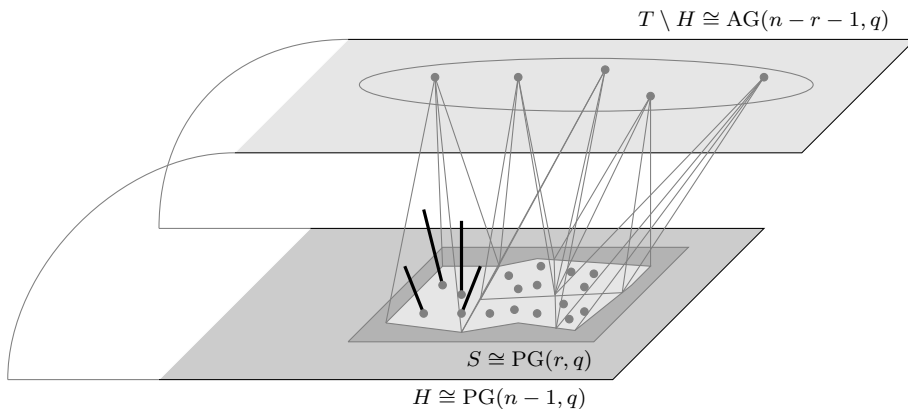


Fig. 3. General construction for affine blocking sets

An important special case of the theorem is obtained when the arc  $\mathcal{K}$  and the blocking set  $\mathcal{L}$  have the same size.

**Corollary 11.** *Let  $n \geq 3$  be a positive integer and let  $q = p^h$  be a prime power. If there exist*

- an  $(M, w)$ -arc in  $\text{PG}(r, q)$ , for some  $r$  satisfying  $1 \leq r \leq n - 2$ , and
- an  $(M, u)$ -blocking set in  $\text{AG}(n - r - 1, q)$

*then there exists an  $(N, t)$ -blocking set in  $\text{AG}(n, q)$  with*

$$N = qM, \quad t = \min\{M - w, qu\}.$$

The next two examples provide constructions for blocking sets meeting the bound from Theorem 6. These are the first examples of blocking sets lying on the implicit bound from Theorem 6. They exploit the connection between linear codes and (multi)sets of points in finite projective geometries (see also [12, 13, 16]).

**Example 12.** In this example we consider the parameters  $n = 9$ ,  $t = 8$ ,  $q = 8$ . By Theorem 6 (cf. also the tables in [6]) one has that the size of an  $(N, 8)$ -blocking set in

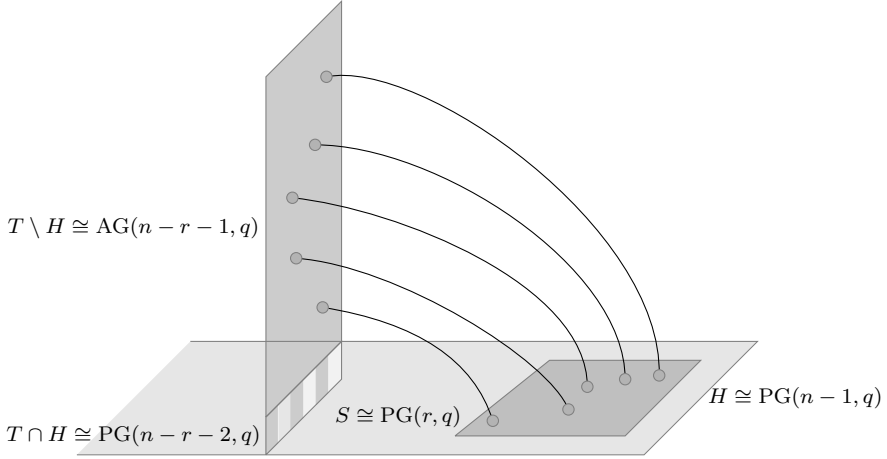


Fig. 4. The construction from Corollary 11

$AG(9, 8)$  is lowerbounded by  $N \geq 120$ . Assume that there exists a  $(119, 8)$ -blocking set in  $AG(9, 8)$ , i.e.  $N = 119, t = 8, n = 9, q = 8$ . Now

$$119 = (t + n + 1 - e)q - n - 1 - \varepsilon = 134 - (8e + \varepsilon),$$

whence  $e = 1, \varepsilon = 7$ . Now by Theorem 6

$$\begin{aligned} 0 &\equiv \sum_{j=0}^8 (-1)^j \binom{-8}{j} \binom{119}{57+7j} \pmod{2} \\ &\equiv \sum_{j=0}^8 \binom{7+j}{j} \binom{119}{57+7j} \pmod{2} \\ &\equiv \binom{119}{57} + \binom{119}{113} \equiv 1 + 0 \pmod{2}, \end{aligned}$$

a contradiction.

We try our construction for different choices of the dimension  $r$ . Let us take  $r = n - 3 = 6$ . For the construction we need an arc in  $PG(6, 8)$  and a blocking set in  $AG(2, q)$ . We take an arc with parameters  $(15, 7)$  associated with the  $[15, 7, 8]_8$ -code which is obtained by shortening the quasicyclic  $[16, 8, 8]_8$ -code (cf. [10]). The blocking set in  $AG(2, q)$  is a  $(15, 1)$ -blocking set, e.g. the union of two nonparallel lines. Now Corollary 11 yields a  $(120, 8)$ -blocking set which meets Ball's lower bound and is therefore optimal.

A possible generalization of this construction would be the following. Take  $q = t = 2^h$ , and  $n = 2^h + 1$ . Now by Theorem 6 there exists no  $(N - 1, t - 1)$  affine blocking set in  $AG(n, q)$  with  $N = 2^{2h+1} - 2^h$ . Thus a hypothetical  $(2^{2h+1} - 2^h, 2^h)$ -blocking set would be optimal. In fact, our construction above solves the case  $h = 3$ . A possible construction would use Corollary 11 with a  $(2^{h+1}, 1)$ -blocking set in  $AG(2, 2^h)$  and a  $(2^{h+1} - 1, 2^h - 1)$ -arc in  $PG(2^h - 2, 2^h)$ . In coding theoretic terms this arc is associated with a code with parameters  $[2^{h+1} - 1, 2^h - 1, 2^h]_{2^h}$ . If we were able to construct linear codes with these

parameters for  $h \geq 4$ , we would immediately get an infinite family blocking sets meeting the implicit Ball bound from Theorem 6.

**Example 13.** In this example, we fix  $q = 4$  and  $n = 4s + 1$ , where  $s \geq 1$  is an integer. We apply Corollary 11 with  $r = 3s - 1$ . Thus for the construction we need an arc  $\mathcal{K}$  in  $\text{PG}(3s - 1, 4)$  and a blocking set  $\mathcal{L}$  in  $\text{AG}(s + 1, 4)$ . A natural choice for  $\mathcal{L}$  is a  $(3s + 4, 1)$ -blocking set meeting Bruen's bound. Such a blocking set does exist in all dimensions. For  $\mathcal{K}$  we would like to have an arc with parameters  $(3s + 4, 3s)$  which is associated with a linear  $[3s + 4, 3s, 4]_4$ -code.

It is known that caps are associated with linear codes of dual distance at least four, i.e. if  $C$  is a linear code associated with a cap then  $d(C^\perp) \geq 4$ . Hence the orthogonal to the codes needed in our construction are  $[3s + 4, 4]_4$ -codes that are associated with caps in  $\text{PG}(3, 4)$ . Since the maximal size of a cap in  $\text{PG}(3, 4)$  is 17, we get codes with the required parameters only if  $3s + 4 \leq 17$ , i.e. for  $s = 1, 2, 3, 4$  (cf. also Grassl's tables [10]). In these four cases Corollary 11 produces a  $(12s + 16, 4)$ -blocking set in  $\text{AG}(4s + 1, 4)$ .

Remarkably, the constructed four blocking sets are optimal. Calculating the conditions of Theorem 6 we obtain that there is no  $(12s + 5, 4)$ -blocking set in  $\text{AG}(4s + 1, 4)$  for  $s = 1, 2, 3, 4$  (the lower bounds for the cases  $s = 1, 2$  are contained also in Table 1 at the end of [6]). Such a blocking set does not exist also for  $s = 5$ . Unfortunately, in this case we cannot construct a  $(76, 4)$ -blocking set from our construction due to the nonexistence of a  $[19, 15, 4]_4$ -code. We can take a  $[20, 15, 4]_4$ -code instead and get a  $(80, 4)$ -blocking set which lies relatively close to the lower bound of 76.

## REFERENCES

- [1] N. ALON. Combinatorial Nullstellensatz. *Combin. Probab. and Computation*, **8**, no. 1–2 (1999), 7–29.
- [2] S. BALL. On intersection sets in Desarguesian affine spaces. *European J. Comb.*, **21** (2000), 441–446.
- [3] S. BALL. On sets of vectors of a finite vector space in which every subset of basis size is a basis. *J. Eur. Math. Soc.*, **14** (2012) 733–748.
- [4] S. BALL, J. DE BEULE. On sets of vectors of a finite vector space in which every subset of basis size is a basis II. *Des. Codes Cryptogr.*, **65** (2012) 5–14.
- [5] S. BALL, A. BLOKHUIS. A bound for the maximum weight of a linear code. *SIAM J. Discrete Math.*, **27** (2013) 575–583.
- [6] S. BALL. A p-adic condition on the weight of a codeword of a linear code. *Des. Codes Cryptogr.*, **72** (2014) 177–183.
- [7] A. BLOKHUIS. On multiple nuclei and a conjecture of Lunelli and Sce. *Bull. Belg. Math. Soc. Simon Stevin*, **3** (1994), 349–353.
- [8] A. E. BROUWER, A. SCHRIJVER. The blocking number of an affine space. *J. Combin. Th. Ser. A*, **24** (1978), 251–253.
- [9] A. A. BRUEN. Polynomial multiplicities over finite fields and intersection sets. *J. Comb. Th. Ser. A*, **60** (1992), 19–33.
- [10] M. GRASSL. Code Tables: Bounds on the parameters of various types of codes, <http://codetables.markus-grassl.de>.
- [11] R. JAMISON. Covering finite fields with cosets of subspaces. *J. Comb. Th. Ser. A* / **22** (1977), 253–256.



- [12] I. LANDJEV. Linear codes over finite fields and finite projective geometries. *Discrete Mathematics*, **213** (2000), 211–214.
- [13] I. LANDJEV. The geometric approach to linear codes, in: Finite Geometries (eds A. Blokhuis, J. Hirschfeld, D. Jungnickel, J. Thas), Ser. Developments in Mathematics, 2001, 247–257.
- [14] I. LANDJEV, A. ROUSSEVA. On the sharpness of Bruen’s bound for intersection sets in Desarguesian affine spaces. *Designs, Codes and Cryptography*, **72** (2014), 551–558.
- [15] I. LANDJEV, A. ROUSSEVA. A General Construction for Affine Blocking Sets, *Results in Mathematics* **75** (2020), #142.
- [16] I. LANDJEV, L. STORME. Linear codes and Galois geometries, chapter 8 in: “Current research topics in Galois geometries” (eds. L. Storme and J. De Beule), NOVA Publishers, 2012, 187–214.
- [17] C. ZANELLA. Intersection sets in  $AG(n, q)$  and a characterization of the hyperbolic quadric in  $PG(3, q)$ . *Discrete Math.* **255** (2002), 381–386.