



All minimal $[9, 4]_2$ -codes are hyperbolic quadrics

Valentino Smaldore

Dipartimento di Matematica, Informatica ed Economia, Università degli Studi della Basilicata, Viale dell'Ateneo Lucano 10, 85100 Potenza, Italy
Dipartimento di Tecnica e Gestione dei Sistemi Industriali, Università degli Studi di Padova, Stradella S. Nicola 3, 36100 Vicenza, Italy

ARTICLE INFO

Keywords:

Minimal codes
Strong blocking sets

ABSTRACT

Minimal codes are being intensively studied in last years. $[n, k]_q$ -minimal linear codes are in bijection with strong blocking sets of size n in $PG(k-1, q)$ and a lower bound for the size of strong blocking sets is given by $(k-1)(q+1) \leq n$. In this note we show that all strong blocking sets of length 9 in $PG(3, 2)$ are the hyperbolic quadrics $Q^+(3, 2)$.

1. Introduction

1.1. First definitions

In this section we fix the notation that we will use in the paper and some preliminary results on minimal codes.

Definition 1.1.

- An $[n, k]_q$ -linear code C is a subspace of $\mathbb{F}_q^n$ of dimension k .
- All the elements of C are said *codewords*.
- The (Hamming) support of a vector $(v_1, v_2, \dots, v_n) = v \in \mathbb{F}_q^n$ is $\sigma(v) = \{i | v_i \neq 0\} \subseteq \{1, 2, \dots, n\}$.
- The (Hamming) weight of v is $w(v) = |\sigma(v)|$.
- A Generator matrix G for C is an $k \times n$ matrix over $\mathbb{F}_q$ such that $C = \text{rowspace}(G)$.

In [1], J. L. Massey used *minimal codewords* to determine the access structure in its codebased secret sharing scheme.

Definition 1.2. Let C be an $[n, k]_q$ code. A nonzero codeword $c \in C$ is *minimal* if for every codeword $c' \in C$ such that $\sigma(c') \subseteq \sigma(c)$, $c' = \lambda c$, for some λ in $\mathbb{F}_q^*$. We say that C is *minimal* if all its codewords are minimal.

As it was noticed in [2], minimal codes are in bijection with strong blocking sets in projective spaces. A strong blocking set in $PG(k-1, q)$ is a set of points $\mathcal{M}$ such that, for each hyperplane σ , $\langle \sigma \cap \mathcal{M} \rangle = \sigma$. Strong blocking sets were introduced by A. A. Davydov, M. Giulietti, S. Marcugini and F. Pambianco in [3]. Later, the same concept was also studied by Sz. Fancsali and P. Sziklai in [4], under the name of *generator sets*, by M. Bonini and M. Borello in [5], under the name of *cutting blocking sets*, and by T. Héger, B. Patkós and M. Takáts in [6], under the name of *hyperplane generating set*.

Theorem 1.3 ([2, Theorem 3.4]). Let C be a non-degenerate $[n, k]_q$ -code with generator matrix $G = (G_1, \dots, G_n)$. Let $S = \{G_1, \dots, G_n\}$ be the corresponding point set of $PG(k-1, q)$. Then, C is a minimal code if and only if S is a strong blocking set.

From the previous theorem it follows the correspondence between $[n, k]_q$ -minimal code and strong blocking sets of $PG(k-1, q)$ of size n . We refer the reader to [2] for more details on minimal codes, while we refer to [7] for a more geometrical approach.

1.2. Minimal length of a minimal code

A general problem is to determine the minimal length of a $[n, k]_q$ -minimal code can have, fixing k and q . Equivalently, the problem is to determine the minimum size n of a strong blocking set in $PG(k-1, q)$. In [8], A. Beutelspacher found a lower bound for n , under the hypothesis $k-1 \leq q$. Later, G. N. Alfano, M. Borello, A. Neri and A. Ravagnani extended the result for all values of k and q .

Theorem 1.4 ([9, Theorem 2.14]). Let C be a $[n, k]_q$ -minimal code. Then $n \geq (k-1)(q+1)$.

Corollary 1.5. Let $q = 2$. If n is the size of a strong blocking set in $PG(k-1, 2)$, then $n \geq 3(k-1)$.

2. Minimal strong blocking sets in $PG(3, 2)$

Consider now the projective space $PG(3, 2)$. From Corollary 1.5 we know that the minimum possible size for a strong blocking set is 9. In [2, Example 5.10], is pointed out that a computer search showed that there is only one minimal code of length 9 up to equivalence. Here we prove in terms of minimal strong blocking sets of $PG(3, 2)$. We call

E-mail address: valentino.smaldore@unibas.it.

minimal strong blocking set a strong blocking set S meeting the lower bound given by Theorem 1.4.

It is easy to see that hyperbolic quadrics $Q^+(3, 2)$ are minimal strong blocking sets, i.e. all planar intersections generate the whole plane. The proof is contained also in [2], and belongs to a more general result in [10]. In fact, it is known that plane section of a quadric is a non-degenerate conic, or a degenerate conic consisting on two concurrent lines, and in both cases the whole plane is generated by the intersection.

We now focus on a geometric characterization of minimal strong blocking sets of $PG(3, 2)$

Lemma 2.1. *Consider a minimal strong blocking set S of $PG(3, 2)$.*

- Any projective plane π in $PG(3, 2)$ contains at most 5 points of S .
- If π contains a line of S , then it contains 5 points of S , forming two lines meeting in a point.

Proof.

- Fix a plane π . Since $|S| = 9$, we want to prove that $|S \cap \pi| > 3$. Assume by contradiction that $|S \cap \pi| \leq 3$, then consider the plane σ through the points in $S \cap \pi$. The intersection of σ and π is a line ℓ , and through a ℓ there pass exactly three planes: σ , π and δ . But now $\delta \cap S \subseteq \ell$, which does not generate the whole plane δ .
- Consider a line $\ell \subset S$. Through ℓ there pass the 3 planes σ , π and δ . Since by the previous a plane may not contain more than 5 points of S , and since $|S| = 9$, we have $|S \cap \pi| = |S \cap \sigma| = |S \cap \delta| = 5$. $\square$

Lemma 2.2. *Let S be a minimal strong blocking set of $PG(3, 2)$. Through each point $P \in S$ there pass exactly 2 lines entirely contained in S .*

Proof. Firstly we prove that through P may not pass more than 2 lines of S . Otherwise, say ℓ_1, ℓ_2, ℓ_3 are 3 lines through P contained in S . Now, $|\ell_1 \cup \ell_2 \cup \ell_3| = 7$, and the other 2 points of the minimal strong blocking set S are on two more lines ℓ_4 and ℓ_5 through P . Since P lies on 7 lines, take ℓ_6 and ℓ_7 meeting S only in P . Now the plane $\langle \ell_6, \ell_7 \rangle$ is such that $S \cap \langle \ell_6, \ell_7 \rangle \in \{S \cap \ell_1, S \cap \ell_2, S \cap \ell_3, S \cap \ell_4, S \cap \ell_5\}$, and in all these cases the intersection does not generate $\langle \ell_6, \ell_7 \rangle$. The second step is to prove that through each $P \in S$ there pass at least two lines of S . Since P lies on 7 lines and $|S \setminus \{P\}| = 8$, by counting we see that at least one of the lines through P is entirely contained in S (recall that a projective line in $PG(3, 2)$ has 3 points). Now fix a line $\ell \subset S$, and the 3 planes π_1, π_2 and π_3 through ℓ . Since by Lemma 2.1 $|S \cap \pi_1| = |S \cap \pi_2| = |S \cap \pi_3| = 5$, each of the planes through ℓ contains an other line in S . But we just proved that a point may not lie on 3 lines in S , so taking the 3 points $P_1, P_2, P_3 \in \ell$, we see that, up to a possible permutation on points, through P_i there pass exactly an other line in $S \cap \pi_i$, $i \in \{1, 2, 3\}$. $\square$

We are now ready to prove the main theorem.

Theorem 2.3. *The minimal strong blocking sets of $PG(3, 2)$ are exactly the hyperbolic quadrics $Q^+(3, 2)$.*

Proof. The thesis arises from the characterization given in Lemmas 2.1 and 2.2, together with the known classification of quadrics in [11].¹ $\square$

Remark 2.4. An other proof of the theorem, which does not involve the classification of polar spaces, arises by checking all projectively non-equivalent configurations of 9 points in $PG(3, 2)$. Since $|PG(3, 2)| = 15$, the set X of all possible configurations of 9 points in $PG(3, 2)$ has size $|X| = \binom{15}{9} = 5005$. In $PG(3, 2)$ there are exactly 5 projectively non-equivalent configurations of 9 points, i.e. $PGL(4, 2)$ has exactly 5 orbits on X :

1. 280 hyperbolic quadrics $Q^+(3, 2)$;
2. 105 configurations that consist on a point P and all the other points out of a fixed plane $\pi \ni P$;
3. 420 configurations that consist on a plane π and two points $P, Q \notin \pi$;
4. 1680 configurations that consist on a punctured plane $\pi \setminus \{P\}$ and other 3 points $Q, R, S \notin \pi$ such that $\langle Q, R, S \rangle \cap \pi = \ell \not\ni P$;
5. 2520 configurations that consist on a punctured plane $\pi \setminus \{P\}$ and other 3 points $Q, R, S \notin \pi$ such that $\langle Q, R, S \rangle \cap \pi = \ell \ni P$.

By the Orbit-Stabilizer Theorem we have $\frac{|PGL(4, 2)|}{|PGL^+(4, 2)|} = \frac{20160}{72} = 280$ hyperbolic quadrics. Now we consider the second configuration. The number of point in $|PG(3, 2)|$ is 15 and through each point there pass 7 planes, so the second set has size $7 \cdot 15 = 105$. The third configuration considers the 15 planes and the all possible pairs of points in the remaining $15 - 7 = |PG(3, 2) \setminus \pi|$, so we get $15 \cdot \binom{8}{2} = 420$. Now we consider all the possibilities made of 6 points on a plane π and three points $Q, R, S \notin \pi$. We have 15 planes, and each time we take out P , one of the 7 points of the plane. Moreover, we should consider all the possible triple of the 8 points out of π , so the total number is $15 \cdot 7 \cdot \binom{8}{3} = 5880$. Here we count twice the 1680 configurations as in 4, and we have 2520 configurations as in 5. We are actually considering all the possibilities since $5005 = 280 + 105 + 420 + 1680 + 2520$, we refer to the arXiv version for all explicit calculations. By following the proofs of Lemmas 2.1 and 2.2 we show that configurations 2, 3, 4, 5 may not be a minimal strong blocking set.

3. Conclusion

In this paper we provided examples of strong blocking set of the minimal possible size allowed by Theorem 1.4 in $PG(3, 2)$. From Corollary 1.5 we know that the size of a minimal strong blocking set in a projective $(k-1)$ -dimensional space over $\mathbb{F}_2$ is $3(k-1)$. In the Fano plane we find the trivial 7 configurations of 6 points given by all the point of the plane except one. The following step should rely on $PG(4, 2)$. In this case $n \geq 12$, while, for example, a parabolic quadric $Q(4, 2)$ is a strong blocking set of size 15. Computer-aided search does not show any configuration of 12 points such that the intersection with all hyperplanes generate the whole 3-space, while it is possible to show minimal strong blocking set of size 15 in $PG(5, 2)$.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

- [1] J.L. Massey, Minimal codewords and secret sharing, in: Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory, 1993, pp. 276–279.
- [2] G.N. Alfarano, M. Borello, A. Neri, A geometric characterization of minimal codes and their asymptotic performance, Adv. Math. Commun. 16 (1) (2022) 115–133.
- [3] A.A. Davydov, M. Giulietti, S. Marcugini, F. Pambianco, Linear nonbinary covering codes and saturating sets in projective spaces, Adv. Math. Commun. 5 (1) (2011) 119–147.
- [4] Sz. Fancsali, P. Sziklai, Lines in higgledy-piggledy arrangement, Electron. J. Combin. 21 (2) (2014) P2.56.
- [5] M. Bonini, M. Borello, Minimal linear codes arising from blocking sets, J. Algebraic Combin. 53 (2) (2021) 327–341.
- [6] T. Héger, B. Patkós, M. Takáts, Search problems in vector spaces, Des. Codes Cryptogr. 76 (2) (2015) 207–216.
- [7] T. Héger, Z.L. Nagy, Short minimal codes and covering codes via strong blocking sets in projective spaces, IEEE Trans. Inform. Theory 68 (2) (2022) 881–890.
- [8] A. Beutelspacher, On baer subspaces of finite projective spaces, Math. Z. 184 (3) (1983) 301–319.

¹ We thank the reviewer for the shortcut in the proof of the main theorem.

- [9] G.N. Alfarano, M. Borello, A. Neri, A. Ravagnani, Three combinatorial perspectives on minimal codes, *SIAM J. Discrete Math.* 36 (1) (2022).
- [10] M. Bonini, S. Lia, M. Timpanella, Minimal linear codes from hermitian varieties and quadrics, *App. Algebr. Eng. Comun. Comput.* (2021).
- [11] J.W.P. Hirschfeld, J. Thas, *General Galois Geometry*, Springer-Verlag, London, 2016.