On subspace codes

Antonio Cossidente
Dipartimento di Matematica e Informatica
Università della Basilicata
Contrada Macchia Romana
I-85100 Potenza
Italy
antonio.cossidente@unibas.it
Francesco Pavese
Dipartimento di Matematica e Informatica
Università della Basilicata
Contrada Macchia Romana
I-85100 Potenza
Italy
francesco.pavese@unibas.it

Abstract

It is shown that any projective bundle of $\mathrm{PG}(2,q)$ gives rise to a q–ary $(6, q^6+2q^2+2q+1, 4; 3)$ subspace code.

KEYWORDS: projective bundle; subspace code; Klein quadric; Singer cyclic group.
AMS MSC: 51E15, 05B25

1 Introduction

Let V be a n–dimensional vector space over $\mathrm{GF}(q)$, q any prime power. The set $S(V)$ of all subspaces of V, or subspaces of the projective space $\mathrm{PG}(V)$, forms a metric space with respect to the *subspace distance* defined by $d_s(U,U') = \dim(U+U') - \dim(U \cap U')$. In the context of subspace coding theory, the main problem asks for the determination of the larger lengths of codes in the space $(S(V), d_s)$ (*subspace codes*) with given minimum distance and of course the classification of the corresponding optimal codes. Codes in the projective space and codes in the Grassmannian over a finite field referred to as subspace codes and constant–dimension codes (CDCs), respectively, have been proposed for error control in random linear network coding. A q–ary $(n, M, d; k)$ constant–dimension subspace code is a set $\mathcal{C}$ of k–subspaces of V, where $|\mathcal{C}| = M$ and minimum subspace distance $d_s(\mathcal{C}) = \min\{d_s(U,U') | U, U' \in \mathcal{C}, U \neq U'\} = d$. In a recent paper [4], the authors show that the maximum size of a binary subspace code of packet length $n = 6$, minimum subspace distance $d = 4$ and constant dimension $k = 3$ is $M = 77$. From a projective point of view this result show that the maximum number of planes in $\mathrm{PG}(5,2)$ mutually intersecting in at most one point is 77. In the same paper, the authors, with the aid of a computer, classify all $(6, 77, 4; 3)$ subspace codes into 5 isomorphism types and a computer–free construction of one isomorphism type is provided. This last isomorphism type is then generalized to any q providing a family of q–ary $(6, q^6+2q^2+2q+1, 4; 3)$ subspace codes. In this paper we provide a construction of families of q–ary $(6, q^6+2q^2+2q+1, 4; 3)$ subspace codes including the family constructed in [4]. Our construction relies on the notion of projective bundle in a projective plane.

A *projective bundle* of $\mathrm{PG}(2,q)$ is a family of q^2+q+1 non–degenerate conics of $\mathrm{PG}(2,q)$ mutually intersecting in a point. In other words, the conics in a projective bundle play the role of lines in $\mathrm{PG}(2,q)$, i.e., it is a model of projective plane. For more details on projective bundles, see [1] and references therein.

2 The construction of subspace codes

Let $\mathrm{PG}(3,q)$ be the 3–dimensional projective space over $\mathrm{GF}(q)$, q any prime power. Let π be a plane in $\mathrm{PG}(3,q)$. Let $\mathcal{B}$ be a projective bundle of π. Let us consider the set $\mathcal{H}$ of all hyperbolic quadrics of $\mathrm{PG}(3,q)$ meeting π in exactly a conic of $\mathcal{B}$. The stabilizer G of π in $\mathrm{PGL}(4,q)$ is a group isomorphic to $q^3 : \mathrm{GL}(3,q)$ [2, Table 8.8]. The number of non–degenerate conics in π is $q^5 - q^2$. The stabilizer in G of a non–degenerate conic C of π has order $q^3(q^3-q)(q-1)$. The stabilizer of C in the group $\mathrm{PGO}^+(4,q)$ of a hyperbolic quadric Q of $\mathrm{PG}(3,q)$ on C has order $2(q^3-q)$. It turns out that the number of hyperbolic quadrics of $\mathcal{H}$ through a conic of $\mathcal{B}$ is $q^3(q-1)/2$. It follows that there are $(q^q+q+1)q^3(q-1)/2$ hyperbolic quadrics of $\mathrm{PG}(3,q)$ meeting π in a conic of $\mathcal{B}$. Two hyperbolic quadrics of $\mathcal{H}$, non on the same conic of $\mathcal{B}$, can share at most one line in a regulus, otherwise the involved conics in the bundle should share at least two points. On the other hand, two hyperbolic quadrics of $\mathcal{H}$ have at least one point in common. Under the Klein correspondence between the lines of $\mathrm{PG}(3,q)$ and points of the Klein quadric $\mathcal{K}$, the lines of the plane π correspond to the points of a Greek plane, say g, of $\mathcal{K}$, and the reguli of a hyperbolic quadric correspond to two polar non–degenerate conic sections of $\mathcal{K}$.

The image of $\mathcal{H}$ on the Klein quadric gives rise to a family of non–degenerate planes $P(\mathcal{H})$ of $\mathcal{K}$ (planes meeting $\mathcal{K}$ in a non–degenerate conic) sharing at most one point.

Firstly, we note the following fact. Let C and C' be two conics of $\mathcal{B}$ meeting at the point P. Then, the tangent lines t and t' to C and C' at P, respectively, must be distinct. This follows from an easy counting argument. Assume that t and t' coincide. Through P there are $q+1$ conics of $\mathcal{B}$ covering all points of π. Each of the $q-1$ conics of $\mathcal{B}$ on P distinct from C and C' meets t in at most one further point other than P. This means that on t there should be at least one uncovered point, a contradiction.

Assume that two planes σ_1 and σ_2 of $P(\mathcal{H})$ have one line in common, say ℓ. Then they generate a projective three-space Σ meeting $\mathcal{K}$ in either an hyperbolic quadric, or an elliptic quadric, or a quadratic cone. Let R_1

and R_2 be the reguli in $\mathrm{PG}(3,q)$ corresponding to the conics $\sigma_1 \cap \mathcal{K}$ and $\sigma_2 \cap \mathcal{K}$. Then, R_1 and R_2 belong to a congruence of lines that could be hyperbolic, elliptic (regular spread) or parabolic, respectively [5, p. 7]. if the reguli R_1 and R_2 are on the same conic of $\mathcal{B}$ then they cannot belong to a hyperbolic congruence because the lines of a hyperbolic congruence meet just two lines (the axes of the congruence). On the other hand, they cannot belong to an elliptic congruence. Indeed, in this case all lines of an elliptic congruence meet a line of $\mathrm{PG}(3,q^2)$ (transversal). Finally, the reguli R_1 and R_2 cannot belong to a parabolic congruence because all its lines meet the axis of the congruence. Assume now that R_1 and R_2 are not on the same conic of $\mathcal{B}$. If the line ℓ is secant to $\Sigma \cap \mathcal{K}$ then R_1 and R_2 should share two lines, which is not the case. Assume that $\Sigma \cap \mathcal{K}$ is a hyperbolic quadric. Then the planes $\sigma_1^{\perp}$ and $\sigma_2^{\perp}$ ($\perp$ is the polarity associated with $\mathcal{K}$) have a secant line in common and again this cannot be the case. Assume that ℓ is external to $\Sigma \cap \mathcal{K}$ and that $\Sigma \cap \mathcal{K}$ is an elliptic quadric. Then R_1 and R_2 are disjoint reguli of an elliptic congruence. This is not possible because the relevant hyperbolic quadrics have at least one point in common. Assume that $\Sigma \cap \mathcal{K}$ is a quadratic cone. If ℓ is either tangent or external to $\Sigma \cap \mathcal{K}$ then R_1 and R_2 share one line or none, respectively, and belong to a parabolic congruence with axis m. It follows that m belongs to the opposite reguli of both R_1 and R_2. Then m must pass through the common point, say T, of the two conics in $\mathcal{B}$ intercepted by R_1 and R_2. Note that in a parabolic congruence with axis m there are $q+1$ planes on m and each of them contains (apart from m) other q lines forming a pencil with center on m. There exists a plane σ on m containing q lines on T and hence σ is tangent to both the hyperbolic quadrics of $\mathrm{PG}(3,q)$ arising from R_1 and R_2, at the point T. This means that the two conics of $\mathcal{B}$ intercepted by R_1 and R_2 admit the same tangent line at T, a contradiction. Assume that $\Sigma \cap \mathcal{K}$ is of elliptic type and that ℓ is a tangent line. In this case $\sigma_1^{\perp}$ and $\sigma_2^{\perp}$ share an external line and the three–space they generate meets $\mathcal{K}$ in a quadratic cone. This case has already been considered.

We have proved that $P(\mathcal{H})$ consists of $(q^2+q+1)q^3(q-1) = q^6 - q^3$ non–degenerate planes mutually intersecting in at most one point. By adding to $P(\mathcal{H})$ the other q^3+q^2+q Greek planes of $\mathcal{K}$ distinct from g, we get a family of q^6+q^2+q planes mutually intersecting in at most one point. Indeed, a Greek plane and a non–degenerate plane meet in at most one point since a non–degenerate plane cannot contain a totally singular line. Through a totally singular line r of $\mathcal{K}$ there are $q-1$ planes $\mathcal{K}_r$ of $\mathrm{PG}(5,q)$ meeting $\mathcal{K}$

exactly in r. Varying the line r over the plane g and choosing one of the planes in $\mathcal{K}_r$ we get a family $\mathcal{T}$ of q^2+q+1 planes mutually intersecting in at most one point. Let $\pi_1 \in \mathcal{K}_{r_1}$ and $\pi_2 \in \mathcal{K}_{r_2}$ be planes of $\mathrm{PG}(5,q)$ meeting g in the lines r_1 and r_2, respectively, with $r_1 \neq r_2$. Assume that the planes π_1 and π_2 share a line. Then they generate a projective three–space containing g and therefore another totally singular plane $\bar{g}$ (Latin plane). This means that $\bar{g}$ meets π_1 and π_2 in a totally singular line distinct from r_1 and r_2, respectively, a contradiction. Note that It is always possible to assume that $\mathcal{T}$ is an orbit of a Singer cyclic group of $\mathrm{PGL}(3,q)$. On the other hand a plane of $\mathcal{T}$ cannot meet a Greek plane distinct from g in a line s. If this was the case, s should be on g. Since two Greek planes meet in exactly one point, we get a contradiction. Finally, a plane of $\mathcal{T}$ cannot meet a plane of $P(\mathcal{K})$ in a line r. This follows from the fact that the line r should be tangent to $\mathcal{K}$ in a point of g. On the other hand a plane of $P(\mathcal{H})$ is a conic section of $\mathcal{K}$ disjoint from g. Indeed, no line contained in a hyperbolic quadric of $\mathcal{H}$ lies on π.

We have proved the following theorem

Theorem 2.1. *Any projective bundle of* $\mathrm{PG}(2,q)$ *gives rise to a q–ary* $(6, q^6 + 2q^2 + 2q + 1, 4; 3)$ *subspace code.*

Remark 2.2. Let π_0 be the projective plane $\mathrm{PG}(2,q)$. Embed π_0 into $\pi = \mathrm{PG}(2,q^3)$, and let σ be the period 3 collineation of π fixing π_0. Let us fix a triangle T of vertices P, P^σ, P^{σ^2} in π. Up to date, the known types of projective bundles are as follows [3]:

1. *circumscribed bundle* consisting of all conics of π_0 containing the vertices of T. This exists for all q;
2. *inscribed bundle* consisting of all conics of π_0 that are tangent to the three sides of T. This exists for all odd q;
3. *self–polar bundle* consisting of all conics of π_0 with respect to which T is self–polar. This exists for all odd q.

All these projective bundles are invariant under a Singer cyclic group of $\mathrm{PGL}(3,q)$. The family of q–ary $(6, q^6 + 2q^2 + 2q + 1, 4; 3)$ subspace codes constructed in [4] admits a group of order $3q^3(q^3 - 1)$ that is the normalizer in G of a Singer cyclic group of $\mathrm{GL}(3,q)$.

Acknowledgments. This work has been published in *Des. Codes Cryptogr.* (2016) 78:527-531. DOI 10.1007/s10623-014-0018-6.

References

[1] R.D. Baker, J.M.N. Brown, G.L. Ebert, J.C. Fisher, Projective bundles, *Bull. Belg. Math. Soc. Simon Stevin* 1 (1994), no. 3, 329-336.

[2] J.N. Bray, D.F. Holt, Derek, C.M. Roney–Dougal, *The maximal subgroups of the low-dimensional finite classical groups*, London Mathematical Society Lecture Note Series, 407,Cambridge University Press, Cambridge, 2013.

[3] D.G. Glynn, *Finite projective planes and related combinatorial systems*, Ph.D. thesis, Adelaide Univ., 1978.

[4] T. Honold, M. Kiermaier, S. Kurz, Optimal binary subspace codes of length 6, constant dimension 3 and minimum distance 4, preprint (arXiiv:1311.0464v1).

[5] J.W.P.H. Hirschfeld, *Finite projective spaces of three dimensions*, Oxford Mathematical Monographs, Oxford Science Publications,The Clarendon Press, Oxford University Press, New York, 1985.