21st International Symposium on
Mathematical Theory of Networks and Systems
July 7-11, 2014. Groningen, The Netherlands

Linear codes arising from finite incidence structures

Daniele Bartoli[1] and Leo Storme[2]

Abstract— **Coding theory and the theory of finite projective spaces, also called Galois geometries, are closely linked to each other. A large variety of problems in coding theory can be retranslated into equivalent problems on specific substructures of finite projective spaces. These latter links include functional codes and projective Reed-Muller codes. This talk presents recent results on functional codes and projective Reed-Muller codes, and presents the main ideas and techniques which led to these new results.**

Keywords: Functional codes, Projective Reed-Muller codes, Algebraic varieties, Quadrics
AMS MSC 2010: 05B25, 51E20, 94B05

I. INTRODUCTION

Consider the finite projective space PG(N, q) of dimension N over the finite field $\mathbb{F}_q$ of order q [9], [10].

These finite projective spaces and their substructures are first of all investigated for their geometrical interest. But they are also investigated because of their links to other research areas, such as Coding Theory. These links include the equivalence between linear MDS codes and arcs in finite projective spaces, the equivalence between linear codes meeting the Griesmer bound and minihypers, and the equivalence between covering codes and saturating sets in finite projective spaces [12].

But also a large variety of linear codes exist whose definition arises from well-defined substructures of finite projective spaces. Via the incidence matrices of points and k-spaces of $PG(N, q)$, it is possible to define the generator matrix or the parity check matrix of a linear code C [1].

Also, variations on this theme of using projective spaces to define linear codes occur. These include functional codes and projective Reed-Muller codes [3], [4].

Via geometrical methods, properties of these linear codes are derived. In this way, finite projective spaces contribute in various ways to coding theory.

In this talk, we will present a number of these results, thereby also showing which geometrical ideas are used to obtain these results.

II. FUNCTIONAL CODES FROM A VARIETY AND A QUADRIC

Functional codes were introduced in [11]. In [2], [6], [7], [8], new results on functional codes linked to quadrics and to Hermitian varieties have been obtained. The next step is to investigate functional codes linked to other algebraic varieties.

The research of [4] continues this way. A first natural generalization is to investigate functional codes arising from the intersection of a given non-singular quadric $\mathcal{Q}_N$ with all algebraic varieties of degree $h \geq 3$.

Let $\mathcal{Q}_N$ be a non-singular quadric variety of PG(N, q), $N \geq 6$, $q > 9$. Let $\mathcal{Q}_N = \{P_1, \ldots, P_n\}$, where we normalize the coordinates of these points P_i with respect to the leftmost non-zero coordinate. Let $\mathcal{F}_h$ be the set of all homogeneous polynomials $f(X_0, \ldots, X_N)$, of degree h, defined by $N + 1$ variables over the finite field $\mathbb{F}_q$. The functional code $C_h(\mathcal{Q}_N)$ is the linear code

$$C_h(\mathcal{Q}_N) = \{(f(P_1), \ldots, f(P_n))||f \in \mathcal{F}_h \cup \{0\}\}.$$

The main problem is to determine the minimum distance d of $C_h(\mathcal{Q}_N)$, one of its fundamental parameters. Since this code is linear, its minimum distance corresponds to its minimum weight. The small weight codewords arise from the algebraic varieties of degree h having the largest intersections with $\mathcal{Q}_N$.

D. Bartoli and L. Storme investigated the problem of the minimum weight of $C_h(\mathcal{Q}_N)$, with $h \geq 3$, via geometrical arguments.

For small h, they proved in [4] that the largest intersections of a non-singular quadric $\mathcal{Q}_N$ in PG(N, q), $N \geq 6$, $q > 9$, with the algebraic varieties of degree h are equal to the union of h quadric varieties of dimension $N - 2$.

This is proven in the following way. By Bézout's theorem, a non-singular quadric $\mathcal{Q}_N$ in PG(N, q), $N \geq 6$, $q > 9$, and an algebraic variety of degree h intersect in an algebraic variety of degree $2h$ and dimension $N - 2$. Results by Cafure and Matera [5] give bounds on the number of points in algebraic varieties. These bounds enable to determine that for the small weight codewords of the functional code $C_h(\mathcal{Q}_N)$, this intersection of degree $2h$ and dimension $N-2$ is the intersection of $\mathcal{Q}_N$ with an algebraic variety of degree h equal to the union of h hyperplanes. This important information implies that we can even obtain extra results: the largest intersections arise from the intersection of $\mathcal{Q}_N$ with the union of h hyperplanes passing through a common $(N - 2)$-space.

III. PROJECTIVE REED-MULLER CODES

Let $\theta_n = (q^{n+1} - 1)/(q - 1)$.

Consider the set $\mathbb{F}_q[X_0, \ldots, X_n]_d^h \cup \{0\}$ of all homogeneous polynomials of degree d over the finite field $\mathbb{F}_q$ of order q in the $n+1$ variables $X_0, \ldots, X_n$. Consider also the n-dimensional projective space PG(n, q) over the finite field

[1]Daniele Bartoli is with Department of Mathematics, Ghent University, Krijgslaan 281, 9000 Ghent, Belgium daniele275@gmail.com
[1]Leo Storme is with Department of Mathematics, Ghent University, Krijgslaan 281, 9000 Ghent, Belgium ls@cage.ugent.be

ISBN: 978-90-367-6321-9

of order q, and order the points $P_0, \ldots, P_{\theta_n - 1}$ of PG(n, q) in a certain way, where we normalize the coordinates of the points P_i by making the leftmost non-zero coordinate equal to one.

Then the *d-th order q-ary projective Reed-Muller code* PRM(q, d, n) is the image of the map

$$\Phi : \mathbb{F}_q[X_0, \ldots, X_n]_d^h \cup \{0\} \to \mathbb{F}_q^{\theta_n} :$$
$$F(X_0, \ldots, X_n) \mapsto (F(P_0), \ldots, F(P_{\theta_n - 1})).$$

The non-zero codewords of minimum weight of PRM(q, d, n) correspond to the algebraic hypersurfaces of degree d having the largest number of points.

For $d \leq q - 1$, it is known from results of Sboui that they correspond to the algebraic hypersurfaces which are the union of d hyperplanes passing through a common $(n-2)$-dimensional subspace of PG(n, q) [13].

Other results of Sboui include that if $q > d(d-1)/2$, then any algebraic hypersurface of degree d, not the union of d hyperplanes, contains less points than any algebraic hypersurface which is the union of d hyperplanes.

D. Bartoli, A. Sboui, and L. Storme continued the study of Sboui for $d < \sqrt[3]{q}$. They determined results related to the question how many points an algebraic curve (resp. an algebraic hypersurface) over a finite field can have, depending on its number of lines (resp. hyperplanes).

In [3], they obtained the following results.

Theorem 1: Let c be a non-zero codeword of the d-th order q-ary projective Reed-Muller code PRM(q, d, n), $d < \sqrt[3]{q}$, of weight

(1)
$$w(c) < q^n - \left(\frac{r+d-4}{2}\right) q^{n-1}$$
$$-((d-r+1)^2 + d - r + 2\sqrt{q})q^{n-2}$$
$$-(d + 2\sqrt{q} - r)q^{n-3} - (d - r + 2\sqrt{q})\,\theta_{n-4} - \frac{r-d}{2},$$
when $d - r + 1$ is odd,

(2)
$$w(c) < q^n - (\frac{d+r-3}{2})q^{n-1}$$
$$-\left(\frac{(d-r+1)^2}{2} + d + 1 - r\right) q^{n-2}$$
$$-\left(\frac{3d-3r+3}{2}\right) q^{n-3} - (d-r+1)\theta_{n-4},$$
when $d - r + 1$ is even,

then c corresponds to an algebraic hypersurface of degree d in PG(n, q), containing at least r hyperplanes.

The main techniques involved the following arguments.

First of all, a detailed study of the number of points in PG$(2, q)$, belonging to an algebraic plane curve of degree d, d small, was performed. Using the Hasse-Weil bound, this led to the following result.

Lemma 1: Let C be an algebraic plane curve of degree d in the projective plane PG$(2, q)$, such that $2 \leq d \leq \frac{\sqrt{q}}{2}$ and $q > 13$. If C contains at most r different lines, then $\#C \leq B_r$, where

$$B_r = \begin{cases} \left(\frac{d+r}{2}\right) q + \frac{d-r}{2} + 1, & d - r \text{ even}, \\ \left(\frac{d+r-1}{2}\right) q + 2\sqrt{q} + \frac{d-r+1}{2}, & d - r \text{ odd}. \end{cases}$$

A second argument involved the lines of an absolutely irreducible algebraic hypersurface Φ of degree d, d small, in PG(n, q), passing through a non-singular point P of Φ. These lines all are contained in the tangent hyperplane in P to Φ.

Using upper bounds on the number of points on an algebraic hypersurface in PG$(n-2, q)$, the combination of the arguments implied upper bounds on the number of points of algebraic hypersurfaces of degree $d < \sqrt[3]{q}$ in PG(n, q), containing exactly $r - 1$ hyperplanes.

Theorem 2: Let Φ be an algebraic hypersurface of degree $d < \sqrt[3]{q}$ in PG(n, q), containing exactly $r - 1$ hyperplanes, then

(1)
$$|\Phi| \leq \left(\frac{r+d-2}{2}\right) q^{n-1}$$
$$+((d-r+1)^2 + d - r + 1 + 2\sqrt{q})q^{n-2} +$$
$$(d + 2\sqrt{q} + 1 - r)q^{n-3} + (d + 1 - r + 2\sqrt{q})\,\theta_{n-4} + \frac{r-d}{2},$$
when $d - r + 1$ is odd,

(2)
$$|\Phi| \leq (\frac{d+r-1}{2})q^{n-1}$$
$$+\left(\frac{(d-r+1)^2}{2} + d + 2 - r\right) q^{n-2} +$$
$$\left(\frac{3d-3r+5}{2}\right) q^{n-3} + (d-r+2)\theta_{n-4},$$
when $d - r + 1$ is even.

These bounds then implied the corresponding results for the weights of the codewords of the d-th order q-ary projective Reed-Muller code PRM(q, d, n) of Theorem 1.

REFERENCES

[1] E.F. Assmus and J.D. Key, Designs And Their Codes. Cambridge Tracts in Mathematics 103. Cambridge: Cambridge University Press, 1992.

[2] D. Bartoli, M. De Boeck, S. Fanali, and L. Storme, On the functional codes defined by quadrics and Hermitian varieties, Des. Codes Cryptogr., to appear.

[3] D. Bartoli, A. Sboui, and L. Storme, Bounds on the number of rational points of algebraic hypersurfaces over finite fields, with applications to projective Reed-Muller codes, in preparation.

[4] D. Bartoli and L. Storme, On the functional codes arising from the intersections of algebraic varieties of small degree with a non-singular quadric, Adv. Math. Commun., submitted.

[5] A. Cafure and G. Matera, Improved explicit estimates on the number of solutions of equations over a finite field, Finite Fields Appl., vol. 12, pp. 155–185, 2006.

[6] F.A.B. Edoukou, A. Hallez, F. Rodier, and L. Storme, On the small weight codewords of the functional codes $C_{herm}(\mathrm{X})$, X a non-singular Hermitian variety, Des. Codes Cryptogr., vol. 56, pp. 219–233, 2010.

[7] F.A.B. Edoukou, A. Hallez, F. Rodier, and L. Storme, A study of intersections of quadrics having applications on the small weight codewords of the functional codes $C_2(Q)$, Q a non-singular quadric, J. Pure Applied Algebra, vol. 214, pp. 1729–1739, 2010.

[8] A. Hallez and L. Storme, Functional codes arising from quadric intersections with Hermitian varieties, Finite Fields Appl., vol. 16, pp. 27–35, 2010.

[9] J.W.P. Hirschfeld, Projective Geometries Over Finite Fields, 2nd edition. Oxford Mathematical Monographs. Oxford: Clarendon Press, 1998.

[10] J.W.P. Hirschfeld and J.A. Thas, General Galois Geometries. Oxford Mathematical Monographs. Oxford: Clarendon Press, 1991.

[11] G. Lachaud, Number of points of plane sections and linear codes defined on algebraic varieties, Arithmetic, Geometry, and Coding Theory, (Luminy, France, 1993), Walter De Gruyter, Berlin-New York, pp. 77–104, 1996.

[12] 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, pp. 187–214, 2012.

[13] J.-P. Serre, Lettre à M. Tsfasman du 24 Juillet 1989, in Journées Arithmétiques.