Journal of Algebra 350 (2012) 84–107

Contents lists available at SciVerse ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

The dual minimum distance of arbitrary-dimensional algebraic–geometric codes

Alain Couvreur

INRIA Saclay – École polytechnique, Laboratoire d'informatique (LIX), UMR 7161, 91128 Palaiseau Cedex, France

ARTICLE INFO

Article history:
Received 27 November 2009
Available online 16 November 2011
Communicated by Steven Dale Cutkosky

MSC:
14J20
94B27
14C20

Keywords:
Algebraic geometry
Finite fields
Error-correcting codes
Algebraic–geometric codes
Linear systems

ABSTRACT

In this article, the minimum distance of the dual $C^{\perp}$ of a functional code C on an arbitrary-dimensional variety X over a finite field $\mathbf{F}_q$ is studied. The approach is based on problems *à la Cayley–Bacharach* and consists in describing the minimal configurations of points on X which fail to impose independent conditions on forms of some degree m. If X is a curve, the result improves in some situations the well-known *Goppa designed distance*.

Introduction

A classical problem in coding theory is the estimation of the minimum distance of some code or family of codes constructed on some variety or some family of varieties. For algebraic–geometric codes on curves, one easily gets such a lower bound, frequently called the *Goppa designed distance* (see [12, Definition II.2.4]).

On higher-dimensional varieties, the problem becomes really harder even when the geometry of the involved variety is well understood. This difficulty can be explained by a citation from Little in the introduction of a survey on the topic [9, Chapter 7]: "the first major difference between higher-dimensional varieties and curves is that points on X of dimension $\geqslant 2$ are [...] not divisors". Therefore, if getting the Goppa designed minimum distance is an easy exercise of function fields theory, obtaining any relevant information on the minimum distance of an algebraic–geometric code on

E-mail address: alain.couvreur@inria.fr.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2011.09.030

a higher-dimensional variety (or a family of varieties) is often the purpose of an entire article. For instance, codes on quadrics are studied in [1], some general bounds on codes on arbitrary-dimensional varieties are given in [8] and, in [15], codes on surfaces having a low Neron–Severi rank are studied (the list is far from being exhaustive).

Another kind of codes associated to algebraic varieties can be studied: *the dual of a functional code*. That is, the orthogonal space for the canonical inner product in $\mathbf{F}_q^n$. On a curve X, the dual of a functional code is also a functional code on X (see [12, Proposition II.2.10]). It turns out that this result does not hold for higher-dimensional varieties. Such a difference with codes on curves has been felt by Voloch and Zarzar who noticed it in [14] and then proved in [3, §10] using an elementary example of surface (or a higher-dimensional variety, see [2, Remark II.5.5]).

Therefore, on varieties of dimension greater than or equal to 2, one can say that *a new class of codes appears* and it is natural to wonder if this new class contains good codes. This motivates the study of the parameters of these duals of functional codes on arbitrary-dimensional varieties, which is the purpose of this article.

In the present paper, we translate the problem of finding the dual minimum distance of an algebraic–geometric code into a problem of finding some particular configurations of points in a projective space. In particular, we introduce the elementary notion of *minimally m-linked points* (Definition 2.8), that is sets of points which fail to impose independent conditions on forms of degree m and are minimal for this property. This notion relates to problems *à la Cayley–Bacharach* (see [4]) and is central for the proof of Theorem 3.5, which gives estimates or lower bounds for the minimum distance of the duals of functional codes. From a more geometrical point of view, we give the complete description of minimally m-linked configurations of less than $3m$ points in any projective space. It is stated in [4] that complete intersections provide such configurations. In addition, the authors ask whether these configurations are the only ones. We give a positive answer to this question for configurations of cardinality lower than or equal to $3m$.

From the coding theoretic point of view, the most surprising application of this result is the case when the variety is a plane curve. Indeed, in this situation, since the dual of an algebraic–geometric code on a curve is also an algebraic–geometric code on this curve, the dual minimum distance has a lower bound given by the Goppa designed distance. Therefore, we compare the bound yielded by Theorem 3.5 with the Goppa designed distance. It turns out that our bound is better than Goppa's one in two situations. First, when Goppa's bound is negative and hence irrelevant, since our bound is always positive. Second, if one can check some incidence condition on the points of evaluation, then, one can get a bound which is much better than that of Goppa.

Some proofs of the present paper are long and need the treatment of numerous cases. This is the reason why we chose to study examples of applications of the results (in Section 4) before proving them. The study of configurations of points and linear systems having prescribed points in their base locus is often very technical. For instance see the proof of [5, Proposition V.4.3].

Contents

Section 1 is a brief review on algebraic–geometric codes on curves and arbitrary-dimensional varieties. Section 2 is devoted to the definition of the notion of *m-general* and *minimally m-linked* configurations of points in a projective space. The connection between this notion and the dual minimum distance is explained at the beginning of Section 3. In addition, Section 3 contains the main theorem (Theorem 3.5) and its "geometric version" (Theorem 3.8). Theorem 3.5 gives lower bounds for the minimum distance of the dual of a functional code. Explicit examples of applications of the main theorem are presented in Section 4. In particular the case of codes on plane curves and the improvements of the Goppa designed distance are studied.

Sections 5 to 9 are devoted to the proof of Theorem 3.8. In Section 5, two key tools for this proof, namely Lemma 5.1 and Theorem 5.2 are stated. Lemma 5.1 is a useful trick to handle minimally m-linked configurations of points and Theorem 5.2 is one of the numerous formulations of Cayley–Bacharach theorem. Afterwards, Sections 6 to 9 are devoted to the proofs of some results on configurations of points in projective spaces, yielding the proof of Theorem 3.5.