Available online at www.sciencedirect.com
SCIENCE DIRECT®
Finite Fields and Their Applications 11 (2005) 684–699
FINITE FIELDS AND THEIR APPLICATIONS
http://www.elsevier.com/locate/ffa

Schubert varieties, linear codes and enumerative combinatorics

Sudhir R. Ghorpade[a,*,1], Michael A. Tsfasman[b,c,d,2]

[a] *Department of Mathematics, Indian Institute of Technology Bombay, Powai, Mumbai 400076, India*
[b] *Institut de Mathématiques de Luminy, Case 907, 13288 Marseille, France*
[c] *Independent University of Moscow, Russia*
[d] *Dorbushin Math. Lab., Institute for Information Transmission Problems, Moscow, Russia*

Received 26 May 2003; revised 5 July 2004

Communicated by Oscar Moreno

Available online 3 October 2005

Abstract

We consider linear error correcting codes associated to higher-dimensional projective varieties defined over a finite field. The problem of determining the basic parameters of such codes often leads to some interesting and difficult questions in combinatorics and algebraic geometry. This is illustrated by codes associated to Schubert varieties in Grassmannians, called Schubert codes, which have recently been studied. The basic parameters such as the length, dimension and minimum distance of these codes are known only in special cases. An upper bound for the minimum distance is known and it is conjectured that this bound is achieved. We give explicit formulae for the length and dimension of arbitrary Schubert codes and prove the minimum distance conjecture in the affirmative for codes associated to Schubert divisors.
© 2005 Elsevier Inc. All rights reserved.

Keywords: Grassmannian; Linear codes; Minimum distance; Projective system; Schubert variety

* Corresponding author. Fax: +91 222 5723480.
E-mail addresses: srg@math.iitb.ac.in (S.R. Ghorpade), tsfasman@iml.univ-mrs.fr (M.A. Tsfasman).

1 Partially supported by a ‘Career Award’ grant from AICTE, New Delhi and an IRCC grant from IIT Bombay.

2 Partially supported by the RFBR Grants 99-01-01204, 02-01-01041 and 02-01-22005.

1071-5797/$ - see front matter © 2005 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2004.09.002

1. Introduction

Let $\mathbb{F}_q$ denote the finite field with q elements, and let n, k be integers with $1 \leqslant k \leqslant n$. The n-dimensional vector space $\mathbb{F}_q^n$ has a norm, called *Hamming norm*, which is defined by

$$\|x\| = |\{i \in \{1, \ldots, n\} : x_i \neq 0\}| \quad \text{for } x \in \mathbb{F}_q^n.$$

More generally, if D is a subspace of $\mathbb{F}_q^n$, the *Hamming norm of D* is defined by

$$\|D\| = |\{i \in \{1, \ldots, n\} : \text{ there exists } x \in D \text{ with } x_i \neq 0\}|.$$

A *linear $[n, k]_q$-code* is, by definition, a k-dimensional subspace of $\mathbb{F}_q^n$. The adjective *linear* will often be dropped since in this paper we only consider linear codes. The parameters n and k are referred to as the *length* and the *dimension* of the corresponding code. If C is an $[n, k]_q$-code, then the *minimum distance* $d = d(C)$ of C is defined by

$$d(C) = \min\{\|x\| : x \in C, \ \ x \neq 0\}.$$

More generally, given any positive integer r, the *rth higher weight* $d_r = d_r(C)$ of C is defined by

$$d_r(C) = \min\{\|D\| : D \text{ is a subspace of } C \text{ with } \dim D = r\}.$$

Note that $d_1(C) = d(C)$.

An $[n, k]_q$-code is said to be *nondegenerate* if it is not contained in a coordinate hyperplane of $\mathbb{F}_q^n$. Two $[n, k]_q$-codes are said to be *equivalent* if one can be obtained from another by permuting coordinates and multiplying them by nonzero elements of $\mathbb{F}_q$; in other words, if they are in the same orbit for the natural action of the semidirect product of $(\mathbb{F}_q^*)^n$ and S_n. It is clear that this gives a natural equivalence relation on the set of $[n, k]_q$-codes.

An alternative way to describe codes is via the language of projective systems introduced in [18]. A *projective system* is a (multi)set X of n points in the projective space $\mathbb{P}^{k-1}$ over $\mathbb{F}_q$. We call X *nondegenerate* if these n points are not contained in a hyperplane of $\mathbb{P}^{k-1}$. Two projective systems in $\mathbb{P}^{k-1}$ are said to be *equivalent* if there is a projective automorphism of the ambient space $\mathbb{P}^{k-1}$, which maps one to the other; in other words, if they are in the same orbit for the natural action of $PGL(k, \mathbb{F}_q)$. It is clear that this gives a natural equivalence relation on the set of projective systems of n points in $\mathbb{P}^{k-1}$.

It turns out that a nondegenerate projective system of n points in $\mathbb{P}^{k-1}$ corresponds naturally to a nondegenerate linear $[n, k]_q$-code. Moreover, if we pass to equivalence classes with respect to the equivalence relations defined above, then this correspondence is one-to-one. The minimum distance of the code $C = C_X$ associated to a nondegenerate

Download English Version:

https://daneshyari.com/en/article/9492965

Download Persian Version:

https://daneshyari.com/article/9492965

Daneshyari.com