Linear Algebra and Its Applications 438 (2013) 57–70

Contents lists available at SciVerse ScienceDirect

Linear Algebra and Its Applications

journal homepage: www.elsevier.com/locate/laa

Linearity and complements in projective space

Michael Braun [a], Tuvi Etzion [b,*,1], Alexander Vardy [c,1]

[a] Faculty of Computer Science, University of Applied Sciences Darmstadt, D-64295 Darmstadt, Germany
[b] Department of Computer Science, Technion, Haifa 32000, Israel
[c] Department of Electrical Engineering, University of California San Diego, La Jolla, CA 92093, USA

ARTICLE INFO

Article history:
Received 9 February 2011
Accepted 7 August 2012
Available online 27 September 2012

Submitted by R.A. Brualdi

Keywords:
Network coding
Subspace coding
Complements
Linear codes

ABSTRACT

The projective space of order n over the finite field $\mathbb{F}_q$, denoted here as $\mathbb{P}_q(n)$, is the set of all subspaces of the vector space $\mathbb{F}_q^n$. The projective space can be endowed with distance function $d_S(X, Y) = \dim(X) + \dim(Y) - 2\dim(X \cap Y)$ which turns $\mathbb{P}_q(n)$ into a metric space. With this, *an* (n, M, d) *code* $\mathbb{C}$ *in projective space* is a subset of $\mathbb{P}_q(n)$ of size M such that the distance between any two codewords (subspaces) is at least d. Koetter and Kschischang recently showed that codes in projective space are precisely what is needed for error-correction in networks: an (n, M, d) code can correct t packet errors and ρ packet erasures introduced (adversarially) anywhere in the network as long as $2t + 2\rho < d$. This motivates our interest in such codes.

In this paper, we examine the two fundamental concepts of "complements" and "linear codes" in the context of $\mathbb{P}_q(n)$. These turn out to be considerably more involved than their classical counterparts. These concepts are examined from two different points of view: coding theory and lattice theory. Our results reveal a number of surprising phenomena pertaining to complements and linearity in $\mathbb{P}_q(n)$ and gives rise to several interesting problems.

© 2012 Elsevier Inc. All rights reserved.

1. Introduction

Let $\mathbb{F}_q^n$ be the canonical vector space of dimension n over the finite field $\mathbb{F}_q$ of order q, where q is a prime power. The *projective space* of order n over $\mathbb{F}_q$, denoted herein by $\mathbb{P}_q(n)$, is the set of all

* Corresponding author.
E-mail addresses: michael.braun@h-da.de (M. Braun), etzion@cs.technion.ac.il (T. Etzion), avardy@ucsd.edu (A. Vardy).

[1] This research was supported in part by the United States–Israel Binational Science Foundation (BSF), Jerusalem, Israel, under Grant 2006097.

0024-3795/$ - see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.laa.2012.08.010

the subspaces of $\mathbb{F}_q^n$, including $\{\mathbf{0}\}$ and $\mathbb{F}_q^n$ itself. Given a nonnegative integer $k \leq n$, the set of all subspaces of $\mathbb{F}_q^n$ that have dimension k is known as a *Grassmannian*, and usually denoted by $\mathbb{G}_q(n, k)$. Thus $\mathbb{P}_q(n) = \cup_{0\leq k\leq n}\mathbb{G}_q(n, k)$. It is well known that

$$|\mathbb{G}_q(n, k)| = \begin{bmatrix} n \\ k \end{bmatrix} := \frac{(q^n - 1)(q^{n-1} - 1)\cdots(q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1)\cdots(q - 1)},$$

where $\begin{bmatrix} n \\ k \end{bmatrix}$ is the *q-ary Gaussian coefficient*. It turns out that the natural measure of distance, the *subspace distance* in $\mathbb{P}_q(n)$, is given by

$$d_S(X, Y) := \dim(X) + \dim(Y) - 2\dim(X \cap Y), \tag{1}$$

for all $X, Y \in \mathbb{P}_q(n)$. It is well known (cf. [1,10]) that the function above is a metric; thus both $\mathbb{P}_q(n)$ and $\mathbb{G}_q(n, k)$ can be regarded as metric spaces. Given a metric space, one can define codes. We say that $\mathbb{C} \subseteq \mathbb{P}_q(n)$ is an (n, M, d) *code in projective space* if $|\mathbb{C}| = M$ and $d_S(X, Y) \geq d$ for all $X, Y \in \mathbb{C}$. If an (n, M, d) code $\mathbb{C}$ is contained in $\mathbb{G}_q(n, k)$ for some k, we say that $\mathbb{C}$ is an (n, M, d, k) code. An (n, M, d, k) code is also called a *constant dimension code*.

The (n, M, d), respectively (n, M, d, k), codes in projective space are akin to the familiar codes in the Hamming space, respectively (constant weight) codes in the Johnson space, where the Hamming distance serves as the metric. There are, however, important differences. For all q, n and k, the metric space $\mathbb{G}_q(n, k)$ corresponds to a distance-regular graph, similar to the distance-regular graph resulting from the Johnson space. On the other hand, while the Hamming space $\mathbb{F}_q^n$ is always distance-regular (as a graph), the projective space $\mathbb{P}_q(n)$ is not. This implies that conventional geometric intuition does not always apply.

Codes in $\mathbb{G}_q(n, k)$ were studied, somewhat sparsely, over the past twenty years. For example, the nonexistence of perfect codes in $\mathbb{G}_q(n, k)$ was proved in [3] and again in [12]. In [1] it was shown that "Steiner structures" yield diameter-perfect codes in $\mathbb{G}_q(n, k)$; properties of these structures were studied in [14]. It appears that codes in the projective space $\mathbb{P}_q(n)$ were not studied at all, until recently, e.g., [8–11,16,18].

Recently, Koetter and Kschischang [10] showed that codes in $\mathbb{P}_q(n)$ are precisely what is needed for error-correction in networks: an (n, M, d) code can correct any t packet errors and any ρ packet erasures introduced (adversarially) anywhere in the network as long as $2t + 2\rho < d$. This motivates our interest in such codes.

The well known concept of q-analogs replaces subsets by subspaces of a vector space over a finite field and their sizes by dimensions of the subspaces. In this respect, constant dimension codes are the q-analog of constant weight codes.

The goal of this paper is to examine two basic concepts in coding theory, namely "complements" and "linear codes". These concepts are well-known in coding theory for binary codes and codes over $\mathbb{F}_q$, respectively. Various problems concerning complements of subspaces over $\mathbb{F}_q$ were considered in the past, e.g., [4–6,13]. Our goal is to discuss these concepts in the projective space. We will tackle these concepts from two different points of view, coding theory and lattice theory.

The rest of this paper is organized as follows. In Section 2 we will give a formal definition for the term complement. Four properties will be required. A function which satisfies only some of these properties will be called quasi-complement. We will consider each of the fifteen nonempty subsets of these four properties for the existence of quasi-complements. We will discuss what is the largest subset of $\mathbb{P}_q(n)$ on which a complement function can be defined. In Section 3 we define linear and quasi-linear codes in $\mathbb{P}_q(n)$ and show examples of linear codes of small size. We conjecture and give some evidence that larger codes might not exist. In Section 4 we present our concepts through another point of view, lattice theory. We prove some connection between properties of lattices and quasi-complements. Open problems for further research are presented in Section 5.

Download English Version:

https://daneshyari.com/en/article/6416667

Download Persian Version:

https://daneshyari.com/article/6416667

Daneshyari.com