Finite Fields and Their Applications 45 (2017) 203–216

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Toric codes and finite geometries

John B. Little

Department of Mathematics and Computer Science, College of the Holy Cross, Worcester, MA 01610, United States

ARTICLE INFO

Article history:
Received 21 January 2016
Received in revised form 17 December 2016
Accepted 29 December 2016
Available online 9 January 2017
Communicated by L. Storme

MSC:
primary 94B27
secondary 51C05

Keywords:
Coding theory
Finite geometry
Ring geometry

ABSTRACT

The theory of affine geometries over the rings $\mathbb{Z}/\langle q-1\rangle$ can be used to understand the properties of toric and generalized toric codes over $\mathbb{F}_q$. The standard generator matrices of these codes are produced by evaluating collections of monomials in m variables at the points of the algebraic torus $(\mathbb{F}_q^*)^m$. The exponent vector of such a monomial can be viewed as a point in one of these affine geometries and the minimum distance of the resulting code is strongly tied to the lines in the finite geometry that contain those points. We argue that this connection is, in fact, even more direct than the connection with the lattice geometry of those exponent vectors considered as elements of $\mathbb{Z}^2$ or $\mathbb{R}^2$. This point of view should be useful both as a way to visualize properties of these codes and as a guide to heuristic searches for good codes constructed in this fashion. In particular, we will use these ideas to see a reason why these constructions have been so successful over the field $\mathbb{F}_8$, but less successful in other cases.

© 2017 Elsevier Inc. All rights reserved.

1. Introduction

We will consider a particular construction of linear block codes over a finite field $\mathbb{F}_q$. Mathematically, our codes are simply vector subspaces $C \subset \mathbb{F}_q^n$ whose elements serve as

E-mail address: jlittle@holycross.edu.

http://dx.doi.org/10.1016/j.ffa.2016.12.007

1071-5797/© 2017 Elsevier Inc. All rights reserved.

a set of codewords for representing information. This sort of encoding is done to increase the reliability of communication over noisy channels and has a number of engineering applications. Our standard reference for basic notions and notation in coding theory is [7]. As usual, n always denotes the block length and k denotes the vector space dimension $\dim_{\mathbb{F}_q} C$, so that the set of codewords contains q^k elements. The important parameters of a code are n, k and a third integer d called the minimum Hamming distance. For these linear codes,

$$d = \min_{x \neq 0 \in C} |\{i \mid x_i \neq 0\}|.$$

If we fix n and k, the larger the parameter d is, the larger the error detection and error correction capacity of a code is.

The toric codes studied here are a class of m-dimensional cyclic codes introduced by J. Hansen in [5,6]. (The term “toric code” is also used in another context that has no direct connection with this one.) Hansen uses the geometry of the projective toric variety corresponding to a polytope P in $\mathbb{R}^m$ to describe toric codes, but these may also be understood in a somewhat more concrete way within the general context of evaluation, or functional, codes.

Definition 1.1. Let P be the convex hull of a finite set of integer lattice points, contained in $[0, q-2]^m \subset \mathbb{R}^m$ and let $L = \mathrm{Span}\{x^e : e \in P \cap \mathbb{Z}^m\}$ be the $\mathbb{F}_q$-linear span of the monomials x^e in variables $x_1, \ldots, x_m$ corresponding to the lattice points e in P. The linear block code denoted by $C_P(\mathbb{F}_q)$ is the image of the evaluation mapping on the $\mathbb{F}_q$-rational points in the standard m-dimensional torus over $\mathbb{F}_q$:

$$\begin{aligned} \mathrm{ev} : L &\to \mathbb{F}_q^{(q-1)^m} \\ g &\mapsto (g(p) : p \in (\mathbb{F}_q^*)^m). \end{aligned}$$

The condition that $P \subset [0, q-2]^m$ implies that the x^e are linearly independent as functions on $(\mathbb{F}_q^*)^m$. In terms of generator matrices, this construction can also be described as follows. Let α be a primitive element for $\mathbb{F}_q$. If $f \in \mathbb{Z}^m$ is a vector with $0 \leq f_i \leq q-2$ for all i, let p_f denote the point $p_f = (\alpha^{f_1}, \ldots, \alpha^{f_m})$ in $(\mathbb{F}_q^*)^m$. If $e = (e_1, \ldots, e_m) \in P \cap \mathbb{Z}^m$, write

$$(p_f)^e = (\alpha^{f_1})^{e_1} \cdots (\alpha^{f_m})^{e_m} = \alpha^{\langle f, e \rangle}.$$

Then the standard generator matrix for $C_P(\mathbb{F}_q)$ is the $(\dim_{\mathbb{F}_q} L) \times (q-1)^m$ matrix

$$G = ((p_f)^e),$$

whose rows are indexed by $e \in P \cap \mathbb{Z}^m$, and whose columns are indexed by f or $p_f \in (\mathbb{F}_q^*)^m$. We note that if P is the interval $[0, \ell - 1] \subset \mathbb{R}$, then $C_P(\mathbb{F}_q)$ is simply

Download English Version:

https://daneshyari.com/en/article/5771592

Download Persian Version:

https://daneshyari.com/article/5771592

Daneshyari.com