Finite Fields and Their Applications 40 (2016) 61–72

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Higher Hamming weights for locally recoverable codes on algebraic curves

Edoardo Ballico [1], Chiara Marcolla *

Department of Mathematics, University of Trento, Italy

ARTICLE INFO

Article history:
Received 18 May 2015
Received in revised form 30 November 2015
Accepted 11 March 2016
Available online 25 March 2016
Communicated by Chaoping Xing

MSC:
primary 11G20
secondary 11T71, 14H51, 14H50

Keywords:
Algebraic geometric LRC codes
Higher Hamming weights
Norm-Trace LRC codes

ABSTRACT

We study locally recoverable codes on algebraic curves. In the first part of the manuscript, we provide a bound on the generalized Hamming weight of these codes. In the second part, we propose a new family of algebraic geometric LRC codes, which are LRC codes from the Norm-Trace curve. Finally, using some properties of Hermitian codes, we improve the bounds on the distance proposed in Barg et al. (2015) [1] of some Hermitian LRC codes.

1. Introduction

The v-th generalized Hamming weight $d_v(C)$ of a linear code C is the minimum support size of v-dimensional subcodes of C. The sequence $d_1(C), \ldots, d_k(C)$ of generalized Hamming weights was introduced by Wei [37] to characterize the performance of a linear code on the wire-tap channel of type II. Later, the GHWs of linear codes have been used

* Corresponding author.
E-mail addresses: ballico@science.unitn.it (E. Ballico), chiara.marcolla@unito.it (C. Marcolla).

[1] The first author is partially supported by MIUR and GNSAGA of INdAM (Italy).

http://dx.doi.org/10.1016/j.ffa.2016.03.004

in many other applications regarding the communications, as for bounding the covering radius of linear codes [15], in network coding [26], in the context of list decoding [7,9], and finally for secure secret sharing [18]. Moreover, in [2] the authors show in which way an arbitrary linear code gives rise to a secret sharing scheme, in [16,17] the connection between the trellis or state complexity of a code and its GHWs is found and in [4] the author proves the equivalence to the dimension/length profile of a code and its generalized Hamming weight. For these reasons, the GHWs (and their *extended* version, the *relative* generalized Hamming weights [21,19]) play a central role in coding theory. In particular, generalized and relative generalized Hamming weights are studied for Reed–Muller codes [10,23] and for codes constructed by using an algebraic curve [6] as Goppa codes [24,38], Hermitian codes [12,25] and Castle codes [27].

In this paper, we provide a bound on the generalized Hamming weight of locally recoverable codes on the algebraic curves proposed in [1]. Moreover, we introduce a new family of algebraic geometric LRC codes and improve the bounds on the distance for some Hermitian LRC codes.

Locally recoverable codes were introduced in [8] and they have been significantly studied because of their applications in distributed and cloud storage systems [3,13,32,34,35]. We recall that a code $C \in (\mathbb{F}_q)^n$ has locality r if every symbol of a codeword c can be recovered from a subset of r other symbols of c.

In other words, we consider a finite field $K = \mathbb{F}_q$, where q is a power of a prime, and an $[n, k]$ code C over the field K, where $k = log_q(|C|)$. For each $i \in \{1, \dots, n\}$ and each $a \in K$ set $C(i, a) = \{c \in C \mid c_i = a\}$. For each $I \subseteq \{1, \dots, n\}$ and each $S \subseteq C$ let S_I be the restriction of S to the coordinates in I.

Definition 1. Let C be an $[n, k]$ code over the field K, where $k = log_q(|C|)$. Then C is said to have **all-symbol locality r** if for each $a \in \mathbb{F}_q$ and each $i \in \{1, \dots, n\}$ there is $I_i \subset \{1, \dots, n\} \setminus \{i\}$ with $|I_i| \leqslant r$, such that for $C_{I_i}(i, a) \cap C_{I_i}(i, a') = \emptyset$ for all $a \neq a'$. We use the notation (n, k, r) to refer to the parameters of this code.

Note that if we receive a codeword c correct except for an erasure at i, we can recover the codeword by looking at its coordinates in I_i. For this reason, I_i is called a *recovering set* for the symbol c_i.

Let C be an (n, k, r) code, then the distance of this code has to verify the bound proved in [28,8] that is $d \leqslant n - k - \lceil k/r \rceil + 2$. The codes that achieve this bound with equality are called *optimal* LRC codes [32,34,35]. Note that when $r = k$, we obtain the Singleton bound, therefore optimal LRC codes with $r = k$ are MDS codes.

Layout of the paper This paper is divided as follows. In Section 2 we recall the notions of algebraic geometric codes and the definition of algebraic geometric locally recoverable codes introduced in [1]. In Section 3 we provide a bound on the generalized Hamming weights of the latter codes. In Section 4 we propose a new family of algebraic geometric LRC codes, which are LRC codes from the Norm-Trace curve. Finally, in Section 5 we