Finite Fields and Their Applications 54 (2018) 80–100

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Locally recoverable codes from rational maps

Carlos Munuera [a,1], Wanderson Tenório [b,*,2]

[a] Department of Applied Mathematics, University of Valladolid, Avda Salamanca SN, 47014 Valladolid, Castilla, Spain
[b] Faculdade de Matemática, Universidade Federal de Uberlândia, Av. J. N. Ávila 2121, 38408-902, Uberlândia, MG, Brazil

A R T I C L E   I N F O

Article history:
Received 1 June 2017
Received in revised form 24 April 2018
Accepted 25 July 2018
Available online xxxx
Communicated by Iwan Duursma

MSC:
94B27
11G20
11T71
14G50
94B05

Keywords:
Error-correcting code
Locally recoverable code
Algebraic geometry code
Reed–Muller code
Toric code

A B S T R A C T

Locally recoverable codes are error-correcting codes allowing local recovery of lost encoded data in a codeword. We give a method to construct locally recoverable codes from rational maps between affine spaces, whose fibres are used as recovery sets. The recovery of erasures is carried out by Lagrangian interpolation in general and simply by one addition in some good cases. We first state the general construction of these codes and study its main properties. Next we apply it to several types of codes, including algebraic geometry codes, Reed–Muller, and other related codes. The existence of several recovering sets for the same coordinate and the possibility of recover more than one erasure at the same time are also treated.

* Corresponding author.
E-mail addresses: cmunuera@arq.uva.es (C. Munuera), dersonwt@yahoo.com.br (W. Tenório).

[1] Research supported by Spanish Ministerio de Economía y Competitividad under grant MTM2015-65764-C3-1-P MINECO/FEDER.
[2] Research supported by CNPq-Brazil under grants 159852/2014-5 and 201584/2015-8.

https://doi.org/10.1016/j.ffa.2018.07.005

1. Introduction

Error-correcting codes are used to detect and correct any errors occurred during the transmission of information. A *linear code* of length n over the finite field $\mathbb{F}_q$ is a linear subspace $\mathcal{C}$ of $\mathbb{F}_q^n$. If $\mathcal{C}$ has dimension k and minimum Hamming distance d we say that it is a $[n, k, d]$ code.

Locally recoverable (LRC) error-correcting codes were introduced in [5] motivated by the recent and significant use of coding techniques applied to distributed and cloud storage systems. Roughly speaking, local recovery techniques enable us to repair lost encoded data by a local procedure, which means by making use of small amount of data instead of all information contained in a codeword.

Let $\mathcal{C}$ be a $[n, k, d]$ code over $\mathbb{F}_q$. Given a vector $\mathbf{x} \in \mathbb{F}_q^n$ and a subset $R \subseteq \{1, \ldots, n\}$, we write $\mathbf{x}_R = \mathrm{pr}_R(\mathbf{x})$ and $\mathcal{C}_R = \mathrm{pr}_R(\mathcal{C})$, where pr_R is the projection on the coordinates of R. A coordinate $i \in \{1, \ldots, n\}$ is *locally recoverable with locality* r if there is a *recovering set* $R(i) \subseteq \{1, \ldots, n\}$ with $i \notin R(i)$ and $\#R(i) = r$, such that for any codeword $\mathbf{x} \in \mathcal{C}$, an erasure in position i can be recovered by using the information of $\mathbf{x}_{R(i)}$. That is to say, if for all $\mathbf{x}, \mathbf{y} \in \mathcal{C}$, $\mathbf{x}_{R(i)} = \mathbf{y}_{R(i)}$ implies $x_i = y_i$. The code $\mathcal{C}$ has *all-symbol locality* r if any coordinate is locally recoverable with locality at most r. We use the notation $([n, k], r)$ to refer to the parameters of such a code $\mathcal{C}$.

The notion of local recoverability can be extended in two directions as follows: First it can be desirable to dispose of codes with multiple recovering sets for each coordinate [16]. The code $\mathcal{C}$ is said to have t recovering sets if for each coordinate i there exist disjoint sets $R(i, j)$, $j = 1, \ldots, t$, such that $\#R(i, j) \leq r_j$ and the coordinate x_i can be recovered from the coordinates of $\mathrm{pr}_{R(i,j)}(\mathbf{x})$ for all $\mathbf{x} \in \mathcal{C}$, as above. In this case $\mathcal{C}$ has locality $(r_1, \ldots, r_t)$. The existence of several recovering sets is known as the *availability* problem. Secondly we may need to recover more than one erasure at the same time. We say that $\mathcal{C}$ has the (ρ, r) *locality property* if for each coordinate i there is a subset $\bar{R}(i)$ containing i such that $\#\bar{R}(i) \leq r + \rho - 1$ and $\rho - 1$ erasures in $\mathbf{x}_{\bar{R}(i)}$ can be recovered from the remaining coordinates of $\mathbf{x}_{\bar{R}(i)}$.

It is clear that every code of minimum distance $d > 1$ is in fact an LRC code able to recover $\rho = d - 1$ erasures, simply by taking $\bar{R}(i) = \{1, 2, \ldots, n\}$. But such recovering sets do not fit into the philosophy of local recovery. We are interested in codes allowing smaller recovering sets (in relation to their parameters). It is simple to verify that the (smallest) locality r of an $[n, k, d]$ code $\mathcal{C}$ satisfies $d^\perp - 1 \leq r \leq k$, where $d^\perp$ is the dual distance of $\mathcal{C}$. Furthermore we have the following Singleton-like bound: the locality of $\mathcal{C}$ obeys the relation (see [5])

$$\left\lceil \frac{k}{r} \right\rceil \leq n - k - d + 2. \tag{1}$$

Codes reaching equality are called *Singleton-optimal* (or simply optimal) LRC codes, since they have the best possible relationship between these parameters. The number $\Delta = n - k - d + 2 - \lceil k/r \rceil$ is the *optimal defect* (or simply defect) of $\mathcal{C}$. Similarly we say