Locally Recoverable Algebraic Geometry codes

Carlos Munuera

Universidad de Valladolid

cmunuera@arq.uva.es

Abstract. A Locally Recoverable code is an error-correcting code such that any erasure in a single coordinate of a codeword can be recovered from a small subset of other coordinates. We study Locally Recoverable Algebraic Geometry codes arising from certain curves defined by equations with separated variables. The recovery of erasures is obtained by means of Lagrangian interpolation in general, and simply by one addition in some particular cases.

Locally Recoverable (LRC) codes were introduced motivated by the 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, that is by making use of small amount of data instead of all information contained in a codeword.

Let $\mathcal{C}$ be a linear code of length n, dimension k and minimum distance d over the field $\mathbb{F}_q$. A coordinate $i \in \{1, \ldots, n\}$ is *locally recoverable with locality* r if there is a *recovery set* $R_i \subseteq \{1, \ldots, n\}$ with $i \notin R_i$ and $\#R_i = r$, such that for any two codewords $\mathbf{u}, \mathbf{v} \in \mathcal{C}$, whenever $\pi_i(\mathbf{u}) = \pi_i(\mathbf{v})$ we have $u_i = v_i$, where π_i is the projection on the coordinates of R_i. Under this condition, an erasure at position i of $\mathbf{v}$ can be recovered by using the information given by the coordinates of $\mathbf{v}$ with indices in R_i. The code $\mathcal{C}$ is *locally recoverable with locality* r if any coordinate is locally recoverable with locality at most r.

RS codes have the largest possible locality $r = k$. A variation of RS codes for local recoverability purposes was introduced by Tamo and Barg. These so-called LRC RS codes can have much smaller locality than RS codes. Its length is smaller than the size of $\mathbb{F}_q$. This is a usual fact: for most known optimal codes, the cardinality of the ground field $\mathbb{F}_q$ is larger than the code length n. Then the use of such codes for parctical applications rely on alphabets of large size, what limits its usefulness. Thus the search for long optimal codes has become a challenging problem. A method to obtain long codes is to consider codes from algebraic curves with many rational points. In this way the above construction of LRC RS codes was extended by Barg, Tamo and Vladut to the *LRC Algebraic Geometry (LRC AG) codes*, obtaining larger LRC codes.

In this article we study LRC AG codes coming from curves defined by equations with separated variables $A(Y) = B(X)$, paying special attention to the case in which the degrees of $A(Y)$ and $B(X)$ are coprime. We study also the generalized Hamming weights of these codes, and show how in some special cases the recovery can be done simply by one addition.

Joint work with Wanderson Tenório (Universidade Federal de Mato Grosso) and Fernando Torres (Universidade de Campinas).
Partially founded by grants MTM2015-65764-C3-1-P MINECO/FEDER; and 201584/2015-8, 159852/2014-5, 310623/2017-0 from CNPq-Brazil.