Finite Fields and Their Applications 52 (2018) 319–335

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Algebraic geometric codes on many points from Kummer extensions

D. Bartoli [a], L. Quoos [b,*], G. Zini [c]

[a] *Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Via Vanvitelli 1, 06123 Perugia, Italy*
[b] *Instituto de Matemática, Universidade Federal do Rio de Janeiro, Rio de Janeiro 21941-909, Brazil*
[c] *Dipartimento di Matematica e Informatica "Ulisse Dini", Università degli Studi di Firenze, Viale Morgagni 67/A, 50134 Firenze, Italy*

A R T I C L E   I N F O

Article history:
Received 8 November 2016
Received in revised form 21 December 2017
Accepted 20 April 2018
Available online 9 May 2018
Communicated by Michael Tsfasman

MSC:
11G20
14G50
14H55

Keywords:
Weierstrass semigroups
Algebraic geometric codes
Codes on many points
Kummer extensions

A B S T R A C T

For Kummer extensions defined by $y^m = f(x)$, where $f(x)$ is a separable polynomial over the finite field $\mathbb{F}_q$, we compute the number of Weierstrass gaps at two totally ramified places. For many totally ramified places we give a criterion to find pure gaps at these points and present families of pure gaps. We then apply our results to construct n-points algebraic geometric codes with good parameters.

* Corresponding author.
E-mail addresses: daniele.bartoli@unipg.it (D. Bartoli), luciane@im.ufrj.br (L. Quoos), gzini@math.unifi.it (G. Zini).

https://doi.org/10.1016/j.ffa.2018.04.008
1071-5797/

1. Introduction

In the early eighties tools from algebraic geometry were applied by V. Goppa to construct linear codes using algebraic curves over finite fields, see [8]. Nowadays these codes are called algebraic–geometric codes, AG codes for short. The starting point in the construction of an AG code is a projective, absolutely irreducible, non singular algebraic curve $\mathcal{X}$ of genus $g \geq 1$ defined over the finite field $\mathbb{F}_q$ with cardinality q. Let $F = \mathbb{F}_q(\mathcal{X})$ be its function field with $\mathbb{F}_q$ being the field of constants. Consider $Q_1, \ldots, Q_n$ pairwise distinct rational places on F. Let $D = Q_1 + \cdots + Q_n$ and G be divisors such that Q_i is not in the support of G for $i = 1, \ldots, n$. The linear code $C_\Omega(D, G)$ is defined by

$$C_\Omega(D, G) = \{(\mathrm{res}_{Q_1}(\eta), \ldots, \mathrm{res}_{Q_n}(\eta)) \mid \eta \in \Omega(G - D)\} \subseteq \mathbb{F}_q^n,$$

where $\Omega(G - D)$ is the space of $\mathbb{F}_q$-rational differentials η on $\mathcal{X}$ such that either $\eta = 0$ or $\mathrm{div}(\eta) \succeq G - D$ and $\mathrm{res}_{Q_j}\eta$ is the residue of η at Q_j.

The code $C_\Omega(D, G)$ has length n and dimension $k = i(G - D) - i(G)$ where $i(G)$ denotes the speciality index of the divisor G. We say that $C_\Omega(D, G)$ is an $[n, k, d]$-code where d denotes the minimum distance of the code. One of the main features of this code is that its minimum distance d satisfies the classical Goppa bound, namely

$$d \geq \deg G - (2g - 2).$$

The integer $d^* = \deg G - (2g - 2)$ is usually called the *designed minimum distance*. One way to obtain codes with good parameters is to find codes that improve the designed minimum distance.

If $G = \alpha P$ for some rational place P on F and D is the sum of other rational places on $\mathcal{X}$, then the code $C_\Omega(D, G)$ is called an *one-point AG code*. Analogously, if $G = \alpha_1 P_1 + \cdots + \alpha_n P_n$ for n distinct rational places $P_1, \ldots, P_n$ on $\mathcal{X}$, then $C_\Omega(D, G)$ is called a *n-point AG code*. For a more detailed introduction to AG codes, see [13,21].

For a one-point divisor $G = \alpha P$ on the function field F, Garcia, Kim, and Lax [6,7] improved the designed minimum distance using the arithmetical structure of the Weierstrass semigroup at the rational place P. For a two-point divisor $G = \alpha_1 P_1 + \alpha_2 P_2$, Homma and Kim [11] introduced the notion of pure gaps and obtained similar results. By choosing α_1 and α_2 satisfying certain arithmetical conditions depending on the structure of the Weierstrass semigroup at P_1 and P_2, they improved the designed minimum distance. Matthews [17] showed that for an arbitrary curve there exist two-point AG codes that have better parameters than any comparable one-point AG code constructed from the same curve. Finally, for divisors $G = \alpha_1 P_1 + \cdots + \alpha_n P_n$ at n distinct rational places on $\mathcal{X}$, results from the theory of generalized Weierstrass semigroups and pure gaps were obtained by Carvalho and Torres [2]. They have been used to obtain AG codes whose minimum distance beats the classical Goppa bound on the minimum distance, see Theorem 2.4.