Finite Fields and Their Applications 40 (2016) 110–125

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Deep holes in Reed–Solomon codes based on Dickson polynomials

Matt Keti *, Daqing Wan

Department of Mathematics, University of California Irvine, CA 92697-3875, USA

A R T I C L E I N F O

Article history:
Received 18 July 2015
Received in revised form 3 March 2016
Accepted 11 March 2016
Available online 25 April 2016
Communicated by Rudolf Lidl

MSC:
11P05
11T06
11T24
11T71

Keywords:
Character sum
Deep hole
Dickson polynomial
Reed–Solomon code
Subset sum
Waring's problem

A B S T R A C T

For an $[n, k]$ Reed–Solomon code $\mathcal{C}$, it can be shown that any received word r lies a distance at most $n - k$ from $\mathcal{C}$, denoted $d(r, \mathcal{C}) \leq n - k$. Any word r meeting the equality is called a deep hole. Guruswami and Vardy (2005) showed that for a specific class of codes, determining whether or not a word is a deep hole is NP-hard. They suggested passingly that it may be easier when the evaluation set of $\mathcal{C}$ is large or structured. Following this idea, we study the case where the evaluation set is the image of a Dickson polynomial, whose values appear with a special uniformity. To find families of received words that are not deep holes, we reduce to a subset sum problem (or equivalently, a Dickson polynomial-variation of Waring's problem) and find solution conditions by applying an argument using estimates on character sums indexed over the evaluation set.

1. Introduction

Reed–Solomon error-correcting codes are used routinely in technological applications when there is a risk for transmitted data to be lost or corrupt. The classical set-up fixes

* Corresponding author.
E-mail addresses: mketi@uci.edu (M. Keti), dwan@math.uci.edu (D. Wan).

http://dx.doi.org/10.1016/j.ffa.2016.03.005
1071-5797/© 2016 Published by Elsevier Inc.

a finite field $\mathbb{F}_q$, message block length k, and subset of $\mathbb{F}_q$ of size $n > k$ denoted $D = \{x_1, x_2, \dots, x_n\}$. D is often referred to as the evaluation set with typical choices $D = \mathbb{F}_q$ or $\mathbb{F}_q^*$. A message $(m_0, m_1, \dots, m_{k-1})$ is represented by the polynomial $m(x) = m_0 + m_1 x + \dots + m_{k-1}x^{k-1}$. The message is encoded by calculating $(m(x_1), m(x_2), \dots, m(x_n))$, called a codeword. The set of all possible encoded messages is defined as the codebook and is denoted by $\mathcal{C}$.

Let $a = (a_1, a_2, \dots, a_n)$ and $b = (b_1, b_2, \dots, b_n)$ be two words. Define the Hamming distance $d(a, b)$ as the number of coordinates in which a and b differ. The distance between a word u and the codebook $\mathcal{C}$ is defined as $d(u, \mathcal{C}) = \min_{v\in\mathcal{C}} d(u, v)$. It is well known that for Reed–Solomon codes, $d(u, \mathcal{C}) \le n - k$ for any received word u. In studying the error-correcting capacity for Reed–Solomon codes, Guruswami and Vardy in [7] found that for a special family of codes with a small evaluation set, determining whether or not $d(u, \mathcal{C}) = n - k$ for a given u is NP-hard. Any word u satisfying the equality is called a deep hole and they suggested in passing that finding deep holes might be easier when the evaluation set is large. We will further investigate the problem of finding deep holes.

2. Overview of previous work

One way to measure $d(u, \mathcal{C})$ is to run Lagrange Interpolation on the word $u = (u_1, \cdots, u_n)$ to get a fitted polynomial $u(x)$ satisfying $u(x_i) = u_i$ for all $1 \le i \le n$. Then, if $\deg u(x) \le k-1$, then u is a codeword and $d(u, \mathcal{C}) = 0$. Otherwise, $k \le \deg u(x) \le n-1$, and Li and Wan in [12] gave the bound

$$n - \deg u(x) \le d(u, \mathcal{C}) \le n - k$$

which shows that if $\deg u(x) = k$, then u is automatically a deep hole. Many of the results toward the deep hole problem are geared toward examining families of words by degree.

2.1. For $D = \mathbb{F}_q$

The choice of $D = \mathbb{F}_q$ is referred to as a standard Reed–Solomon code. Cheng and Murray in [3] searched for deep holes in this context, and conjectured that the only deep holes were those satisfying $\deg u(x) = k$. More precisely,

Conjecture *(Cheng–Murray). All deep holes for standard Reed–Solomon codes are those words u satisfying* $\deg u(x) = k$.

They weren't able to prove this, but they were able to reduce the problem to finding a rational point on an algebraic hypersurface to derive the first result on deep holes for Reed–Solomon codes over prime field $\mathbb{F}_p$: