ELSEVIER

CrossMark

Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in DISCRETE MATHEMATICS

Electronic Notes in Discrete Mathematics 57 (2017) 33–38

www.elsevier.com/locate/endm

On Syndrome Decoding of Punctured Reed-Solomon and Gabidulin Codes

Hannes Bartz[1], Vladimir Sidorenko[2,3]

Institute for Communications Engineering
Technical University of Munich
D-80290 Munich, Germany

Abstract

Punctured Reed-Solomon (RS) and Gabidulin (G) codes over the field $\mathbb{F}_{q^m}$ *with locators from the subfield* $\mathbb{F}_q$ can be represented as interleaving of m correspondent codes over the subfield $\mathbb{F}_q$ or can be considered as virtual interleaving of m correspondent codes over the field $\mathbb{F}_{q^m}$. Using a probabilistic unique syndrome decoder, m-interleaved or virtually interleaved codes can be decoded up to *the same* radius $\frac{m}{m+1}(d-1)$, where d is the code distance in Hamming metric for RS codes and in rank metric for G codes. We show that the correspondent decoders over the subfield $\mathbb{F}_q$ and the field $\mathbb{F}_{q^m}$ are equivalent and conclude that in practice one should use a decoder over the subfield since it has less complexity.

Keywords: Reed-Solomon, Gabidulin, codes, punctured, interleaved, syndrome decoding.

[1] Email: `hannes.bartz@tum.de`

[2] Email: `vladimir.sidorenko@tum.de`

[3] V. Sidorenko is on leave from the Institute for Information Transmission Problems, Russian Academy of Sciences.

http://dx.doi.org/10.1016/j.endm.2017.02.007

1 Introduction

Reed-Solomon (RS) and Gabidulin (G) codes belong to the family of *evaluation* codes and are widely used for error correction in many applications. An evaluation code over the finite field $\mathbb{F}_{q^m}$ is constructed by evaluating all polynomials with coefficients from $\mathbb{F}_{q^m}$ of restricted degree at a set of code locators. By choosing the code locators from the subfield $\mathbb{F}_q$ we obtain a *punctured* evaluation code over $\mathbb{F}_{q^m}$ which can be equivalently interpreted as an *m-interleaved code $\mathcal{I}$* over the subfield $\mathbb{F}_q$ [1].

It is known that m-interleaved RS and G codes over $\mathbb{F}_q$ with distance d can correct with high probability up to $\frac{m}{m+1}(d-1)$ errors in the corresponding metric [2]. In [3,4] it was shown that the same decoding radius can be achieved by computing element-wise q-powers of the received word at the decoder. This results in a received word V of a *virtually m-interleaved code $\mathcal{V}$* over the large field $\mathbb{F}_{q^m}$. Virtual interleaving with usual powers was proposed already in 2010 and was modified to q-powers in [3].

In this paper we analyze and compare probabilistic unique syndrome-based decoding algorithms for interleaved and virtually interleaved RS and G codes. We show that the syndrome-based decoder of the code $\mathcal{I}$ over the subfield $\mathbb{F}_q$ is *equivalent* to the respective decoder of $\mathcal{V}$ in the field $\mathbb{F}_{q^m}$. This means, that for the same input the decoders return the same output and shows, that the decoding failure probability is the same for both decoders. It allows us to choose the decoder with the lowest computational complexity, i.e., the respective decoder over the subfield $\mathbb{F}_q$. The extended version of the paper with proofs, details and with more references is available online at http://goo.gl/NL78P5.

2 Preliminaries

Let $\mathbb{F}_h$ be a finite field, where h is a power of a prime. Let $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$ be extensions of $\mathbb{F}_h$. By the column vector $\underline{a} = \left(a^{(0)} a^{(1)} \dots a^{(m-1)}\right)^T \subset \mathbb{F}_q^m$ we denote the expansion of an element $a \in \mathbb{F}_{q^m}$ w.r.t. a fixed basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Given a vector $\boldsymbol{a}$ of length n over $\mathbb{F}_{q^m}$, we introduce the $m \times n$ expansion matrix over $\mathbb{F}_q$ as $\underline{\boldsymbol{a}} = (\underline{a_0}, \dots, \underline{a_{n-1}})$.

By $\mathbb{F}_{q^m}[x]$ we denote the ring of all polynomials $g(x) = \sum_{i=0}^{d} g_i x^i$ over $\mathbb{F}_{q^m}$ and $\mathbb{F}_{q^m}[x]_{<k}$ is the set of all polynomial from $\mathbb{F}_{q^m}[x]$ with degree less than k.

A nonzero polynomial of the form $p(x) = \sum_{i=0}^{d} p_i x^{[i]}$, where $[i]$ denotes the i-th Frobenius power $[i] = h^i$, with $p_i \in \mathbb{F}_{q^m}$, $p_d \neq 0$, is called an *h-linearized polynomial* of h-degree $\deg_h(p(x)) = d$. By $\mathbb{L}_{q^m}[x]$ we denote the ring of all h-linearized polynomials over $\mathbb{F}_{q^m}$ and $\mathbb{L}_{q^m}[x]_{<k}$ denotes the set of