Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in DISCRETE MATHEMATICS

Electronic Notes in Discrete Mathematics 57 (2017) 175–180 www.elsevier.com/locate/endm

Decoding Interleaved Gabidulin Codes using Alekhnovich's Algorithm

Sven Puchinger[a], Sven Müelich[a], David Mödinger[b], Johan Rosenkilde né Nielsen[c] and Martin Bossert[a 1]

[a] *Institute of Communications Engineering, Ulm University, Ulm, Germany*

[b] *Institute of Distributed Systems, Ulm University, Ulm, Germany*

[c] *Department of Applied Mathematics & Computer Science, Technical University of Denmark, Lyngby, Denmark*

Abstract

We prove that Alekhnovich's algorithm can be used for row reduction of skew polynomial matrices. This yields an $O(\ell^3 n^{(\omega+1)/2} \log(n))$ decoding algorithm for ℓ-Interleaved Gabidulin codes of length n, where ω is the matrix multiplication exponent.

Keywords: Gabidulin Codes, Characteristic Zero, Low-Rank Matrix Recovery

1 Introduction

It is shown in [1] that *Interleaved Gabidulin codes* of *length* $n \in \mathbb{N}$ and *interleaving degree* $\ell \in \mathbb{N}$ can be error- and erasure-decoded by transforming the

[1] Email: sven.puchinger@uni-ulm.de, sven.mueelich@uni-ulm.de, david.moedinger@uni-ulm.de, jsrn@jsrn.dk, martin.bossert@uni-ulm.de,

http://dx.doi.org/10.1016/j.endm.2017.02.029

following *skew polynomial* [2] matrix into *weak Popov form* (cf. Section 2) [2]:

$$\mathbf{B} = \begin{bmatrix} x^{\gamma_0} & s_1 x^{\gamma_1} & s_2 x^{\gamma_2} & \dots & s_\ell x^{\gamma_\ell} \\ 0 & g_1 x^{\gamma_1} & 0 & \dots & 0 \\ 0 & 0 & g_2 x^{\gamma_2} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & g_\ell x^{\gamma_\ell} \end{bmatrix}, \tag{1}$$

where the skew polynomials $s_1, \dots, s_\ell, g_1, \dots, g_\ell$ and the non-negative integers $\gamma_0, \dots, \gamma_\ell$ arise from the decoding problem and are known at the receiver. Due to lack of space, we cannot give a description of Interleaved Gabidulin codes, the mentioned procedure and the resulting decoding radius here and therefore refer to [1, Section 3.1.3]. By adapting row reduction [3] algorithms known for polynomial rings $\mathbb{F}[x]$ to skew polynomials, a decoding complexity of $O(\ell n^2)$ can be achieved [1]. In this paper, we adapt Alekhnovich's algorithm [7] for row reduction of $\mathbb{F}[x]$ matrices to the skew polynomial case.

2 Preliminaries

Let $\mathbb{F}$ be a finite field and σ an $\mathbb{F}$-automorphism. A *skew polynomial ring* $\mathbb{F}[x, \sigma]$ [2] contains polynomials of the form $a = \sum_{i=0}^{\deg a} a_i x^i$, where $a_i \in \mathbb{F}$ and $a_{\deg a} \neq 0$ ($\deg a$ is the *degree* of a), which are multiplied according to the rule $x \cdot a = \sigma(a) \cdot x$, extended recursively to arbitrary degrees. This ring is non-commutative in general. All polynomials in this paper are skew polynomials.

It was shown in [6] for linearized polynomials and generalized in [3] to arbitrary skew polynomials that two such polynomials of degrees $\leq s$ can be multiplied with complexity $\mathcal{M}(s) \in O(s^{(\omega+1)/2})$ in operations over $\mathbb{F}$, where ω is the matrix multiplication exponent.

A polynomial a has *length* $\operatorname{len} a$ if $a_i = 0$ for all $i = 0, \dots, \deg a - \operatorname{len} a$ and $a_{\deg a - \operatorname{len} a + 1} \neq 0$. We can write $a = \tilde{a} x^{\deg a - \operatorname{len} a + 1}$, where $\deg \tilde{a} \leq \operatorname{len} a$, and multiply $a, b \in \mathbb{F}[x, \sigma]$ by $a \cdot b = [\tilde{a} \cdot \sigma^{\deg a - \operatorname{len} a + 1}(\tilde{b})] x^{\deg a + \deg a - \operatorname{len} a - \operatorname{len} b + 1}$. Computing $\sigma^i(\alpha)$ with $\alpha \in \mathbb{F}$, $i \in \mathbb{N}$ is in $O(1)$ (cf. [3]). Hence, a and b of length s can be multiplied in $\mathcal{M}(s)$ time, although possibly $\deg a, \deg b \gg s$.

Vectors $\mathbf{v}$ and matrices $\mathbf{M}$ are denoted by bold and small/capital letters. Indices start at 1, e.g. $\mathbf{v} = (v_1, \dots, v_r)$ for $r \in \mathbb{N}$. $\mathbf{E}_{i,j}$ is the matrix containing only one non-zero entry $= 1$ at position (i, j) and $\mathbf{I}$ is the identity matrix. We denote the ith row of a matrix $\mathbf{M}$ by $\mathbf{m}_i$. The degree of a vector $\mathbf{v} \in \mathbb{F}[x, \sigma]^r$ is the maximum of the degrees of its components $\deg \mathbf{v} = \max_i \{\deg v_i\}$ and

[2] Afterwards, the corresponding information words are obtained by ℓ many divisions of skew polynomials of degree $O(n)$, which can be done in $O(\ell n^{(\omega+1)/2} \log(n))$ time [3].

[3] By row reduction we mean to transform a matrix into weak Popov form by row operations.