Decoding Square–Free Goppa Codes over $\mathbb{F}_p$

Paulo Barreto, Richard Lindner, Rafael Misoczki

Overview

TECHNISCHE UNIVERSITÄT DARMSTADT

Decoding Square-Free Goppa Codes

Generalized Srivastava Codes

Overview

Decoding Square-Free Goppa Codes

Generalized Srivastava Codes

Goppa Codes over $\mathbb{F}_p$

Let

p be prime, $q = p^m$

$g(x) \in \mathbb{F}_q[x]$ be monic polynomial, $t = \deg(g)$

$L \subseteq \mathbb{F}_q{}^* \setminus \{x : g(x) = 0\}$ be indexed subset, $n = |L|$

Then

$\Gamma_q(L,g) = \{ w \in \mathbb{F}_p{}^n : s_w(x) = 0 \}$ Goppa Code

$s_w(x) = \sum w_i / (x - L_i) \bmod g(x)$ Syndrome

$s_{v+w}(x) = s_v(x) + s_w(x)$

Error-Correction Capabilities

Decoder	Requirement	Capability
Alternant		$t/2$
Patterson	$p=2$, $g(x)$ sf	t
List	$p=2$, $g(x)$ sf	$n - \sqrt{n(n - 2t)}$
Wild	$g(x)=h(x)^{q-1}$, $h(x)$ sf	$qt/2(q-1)$
Wild-List	$g(x)=h(x)^{q-1}$, $h(x)$ sf	$n - \sqrt{n(n - qt/(q-1))}$
New	$g(x)$ sf	$2t/p$

Error-Correction Capabilities

TECHNISCHE UNIVERSITÄT DARMSTADT

Decoder	Requirement	Capability
Alternant		$t/2$
Patterson	$p=2$, $g(x)$ sf	t
List	$p=2$, $g(x)$ sf	$n - \sqrt{(n(n-2t))}$
Wild	$g(x)=h(x)^{q-1}$, $h(x)$ sf	$qt/2(q-1)$
Wild-List	$g(x)=h(x)^{q-1}$, $h(x)$ sf	
New	$g(x)$ sf	$2t/p$

With high prob

Patterson's Decoder I

TECHNISCHE UNIVERSITÄT DARMSTADT

Decoding: Given $w = c + e$ or $s_w(x) = s_e(x)$ find e

$\sigma_e(x) = \prod (x - L_i)^{e_i}$	Error Locator
$\sigma_e'(x) = \sigma_e(x)\, s_e(x) \bmod g(x)$	Key Equation
$\sigma_e(x) = a_0(x)^2 + x\, a_1(x)^2$	Char p=2

$$a_1(x)^2 = (a_0(x)^2 + x\, a_1(x)^2)\, s_e(x) \bmod g(x)$$

$$a_0(x) = a_1(x) \sqrt{(x + 1/s_e(x))} + \lambda(x)\, g(x)$$

$$\nu(x) = \sqrt{(x + 1/s_e(x))}$$

Patterson's Decoder II

TECHNISCHE UNIVERSITÄT DARMSTADT

Decoding: Given $w = c + e$ or $s_w(x) = s_e(x)$ find e

$\ldots\sigma_e(x) = \prod (x - L_i)^{e_i}$

$\ldots a_0(x) = a_1(x)\,\nu(x) + \lambda(x)\,g(x)$

Recover a_0, a_1 such that
$\deg(a_0(x)^2 + x\,a_1(x)^2) \le t$

Unique since mindist $\geq$ 2t+1

Set $\sigma(x) = a_0(x)^2 + x\,a_1(x)^2$
$\sigma(L_i) = 0$ iff $e_i = 1$

Crucial Parts

...$a_0(x) = a_1(x)\,\nu(x) + \lambda(x)\,g(x)$

...Recover a_0, a_1 such that
$\deg(a_0(x)^2 + x\,a_1(x)^2) \leq t$

Find vector of “small degrees” in $\mathbb{F}_q[x]$-module
spanned by

$$\begin{pmatrix} g(x) & 0 \\ \nu(x) & 1 \end{pmatrix}$$

Easy problem: Compute Weak-Popov Form [MS02]

New Decoder for p = 3

TECHNISCHE UNIVERSITÄT DARMSTADT

$$\sigma_e(x) = a_0(x)^3 + x\, a_1(x)^3 + x^2\, a_2(x)^3$$

$$a_0(x) = a_1(x)\, \nu_1(x) + a_2(x)\, \nu_2(x) + \lambda(x)\, g(x)$$

$$\nu_k(x) = -(x^k + k\, x^{k-1}/s_e(x))^{1/3}$$

Compute Weak Popov Form of

$$\begin{bmatrix} g(x) & 0 & 0 \\ \nu_1(x) & 1 & 0 \\ \nu_2(x) & 0 & 1 \end{bmatrix}$$

WPF can be computed efficiently for this structure

New Decoder Capability I

TECHNISCHE UNIVERSITÄT DARMSTADT

Will correct ϵ = wt(e) errors if

1st deg(σ_e(x)) $\leq$ t

One more trick

2nd For all codewords c' $\neq$ c
wt(c - c') $\geq 2\epsilon + 1$

With high prob

New Decoder Capability II

Go through process with all $\phi \in \mathbb{F}_p^*$ and

$\sigma_{\phi,e}(x) = \prod (x - L_i)^{e_i / \phi}$

Best case:

All error magnitudes e_i coincide with some ϕ

$\deg(\sigma_{\phi,e}(x)) = \epsilon \leq t$

We can decode $\epsilon = t$ errors

Occurs for CCA2 transform of McEliece [FO01]

New Decoder Capability III

Go through process with all $\phi \in \mathbb{F}_p^*$ and

$\sigma_{\phi,e}(x) = \prod (x - L_i)^{e_i / \phi}$

Worst-case:

All error magnitudes occur equally often

$\deg(\sigma_{\phi,e}(x)) = (1 + \ldots + p-1)\, \epsilon/(p-1) = \epsilon\, p/2 \leq t$

Can correct $\epsilon = 2t/p$ errors with high prob

Overview

Decoding Square-Free Goppa Codes

Generalized Srivastava Codes

Overview

Decoding Square-Free Goppa Codes

Generalized Srivastava Codes

Tzeng-Zimmermann Form

Theorem [TZ75]:

Any Goppa code Γ_q (L,g) with $g(x) = \prod (x - \alpha_i)^{r_i}$

has party check matrix

$$H = \begin{matrix} H_1 \\ H_2 \\ \dots \\ H_s \end{matrix} \qquad H_i = \begin{matrix} (\alpha_i - L_1)^{-1} & \dots & (\alpha_i - L_n)^{-1} \\ \dots & & \dots \\ (\alpha_i - L_1)^{-r_i} & \dots & (\alpha_i - L_n)^{-r_i} \end{matrix}$$

Generalized Srivastava Codes

Fix t and disjoint tuples of distinct elements

$L_1,\ldots,L_n;\ \alpha_1,\ldots,\alpha_s;\ z_1,\ldots,z_n \in \mathbb{F}_q^*$

Parity check matrix of associated GS code is

$$H = \begin{matrix} H_1 \\ H_2 \\ \ldots \\ H_s \end{matrix} \cdot \mathrm{diag}(z_1,\ldots,z_n) \qquad H_i = \begin{matrix} (\alpha_i - L_1)^{-1} & \ldots & (\alpha_i - L_n)^{-1} \\ \ldots & & \ldots \\ (\alpha_i - L_1)^{-t} & \ldots & (\alpha_i - L_n)^{-t} \end{matrix}$$

Generalized Srivastava Codes

TECHNISCHE UNIVERSITÄT DARMSTADT

Fix t and disjoint tuples of distinct elements

$L_1, \ldots, L_n;\ \alpha_1, \ldots, \alpha_s;\ z_1, \ldots, z_n \in \mathbb{F}_q^*$

Parity check matrix of associated GS code is

H = H_1 H … H_s

Goppa code with L,
$g(x) = \prod (x - \alpha_i)^t$
and fixed transform for each coordinate

… $(\alpha_i - L_n)^{-1}$

…

$(\alpha_i - L_1)^{-t}$ … $(\alpha_i - L_n)^{-t}$

Thank you

Further Questions?