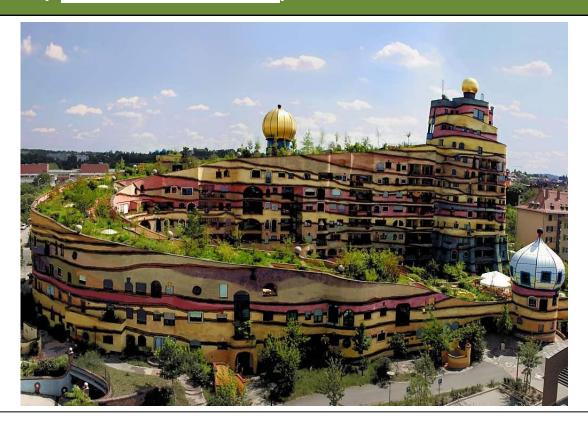
Decoding Square–Free Goppa Codes over \mathbb{F}_p



Paulo Barreto, Richard Lindner, Rafael Misoczki





Decoding Square-Free Goppa Codes



Decoding Square-Free Goppa 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 $s_{w}(x) = \sum w_{i} / (x - L_{i}) \mod g(x)$ Syndrome $s_{v+w}(x) = s_{v}(x) + s_{w}(x)$

Error-Correction Capabilities



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

Error-Correction Capabilities



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

Patterson's Decoder I



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

$$\sigma_{\rm e}({\rm x}) = \prod ({\rm x} - {\rm L_i})^{\rm e_i}$$

$$\sigma_{e}'(x) = \sigma_{e}(x) s_{e}(x) \mod g(x)$$

$$\sigma_{\rm e}({\rm x}) = {\rm a}_0({\rm x})^2 + {\rm x} {\rm a}_1({\rm x})^2$$

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

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

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

Patterson's Decoder II



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

...
$$\sigma_{e}(x) = \prod (x - L_{i})^{e_{i}}$$

... $a_{0}(x) = a_{1}(x) \nu(x) + \lambda(x) g(x)$

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 $deg(a_0(x)^2 + x a_1(x)^2) \le t$

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

Easy problem: Compute Weak-Popov Form

[MS02]

New Decoder for p = 3

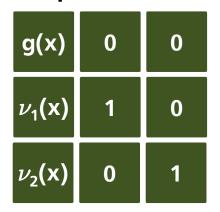


$$\sigma_{\rm e}(x) = a_0(x)^3 + x a_1(x)^3 + x^2 a_2(x)^3$$

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

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

Compute Weak Popov Form of



WPF can be computed efficiently for this structure

New Decoder Capability I



Will correct ϵ = wt(e) errors if

1st $deg(\sigma_e(x)) \leq t$

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

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

Best case:

All error magnitudes e_i coincide with some ϕ $deg(\sigma_{\phi,e}(x)) = \epsilon \le t$

We can decode ϵ = t errors

Occurs for CCA2 transform of McEliece [FO01]

New Decoder Capability III



Go through process with all $\phi \in \mathbb{F}_p^*$ and $\sigma_{\phi,e}(\mathbf{x}) = \prod (\mathbf{x} - \mathsf{L}_i)^{|\mathbf{e}_i|/|\phi}$

Worst-case:

All error magnitudes occur equally often $deg(\sigma_{\phi,e}(x)) = (1 + ... + p-1) \epsilon/(p-1) = \epsilon p/2 \le t$ Can correct $\epsilon = 2t/p$ errors with high prob



Decoding Square-Free Goppa Codes



Decoding Square-Free Goppa Codes

Tzeng-Zimmermann Form



Theorem [TZ75]:

Any Goppa code Γ_q (L,g) with g(x) = \prod (x - α_i)^{r_i} has party check matrix

Generalized Srivastava Codes



Fix t and disjoint tuples of distinct elements

$$L_1,...,L_n$$
; $\alpha_1,...,\alpha_s$; $Z_1,...,Z_n \in \mathbb{F}_q^*$

Parity check matrix of associated GS code is

$$H = \begin{array}{c} H_1 \\ H_2 \\ \dots \\ H_s \end{array} \cdot diag(z_1, \dots, z_n) \qquad H_i = \begin{array}{c} (\alpha_i - L_1)^{-1} \\ \dots \\ (\alpha_i - L_1)^{-1} \\ \dots \\ (\alpha_i - L_1)^{-1} \end{array} \dots \qquad (\alpha_i - L_n)^{-1}$$

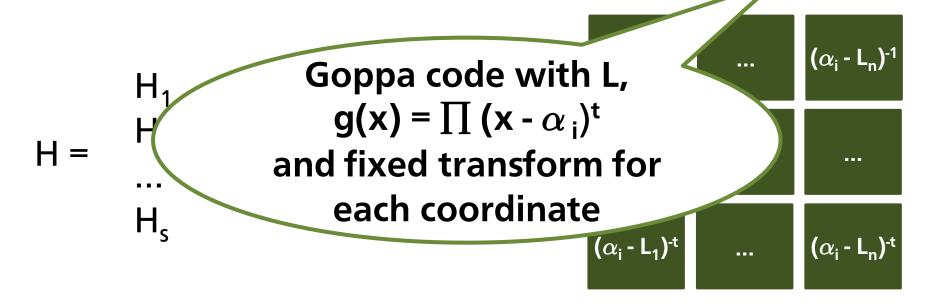
Generalized Srivastava Codes



Fix t and disjoint tuples of distinct elements

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

Parity check matrix of associated GS code is





Thank you

Further Questions?