Power Decoding of Punctured Subspace Codes

Ханнес Бартц[1], Владимир Сидоренко[1,2]

[1]Institute for Communications Engineering (LNT)
Technical University of Munich (TUM)
Munich, Germany

[2]Институт проблем передачи информации (ИППИ)
Москва, Россия

Институт проблем передачи информации (ИППИ), Москва, Россия

4 Октябрь, 2016

Outline

Some Definitions

- $\mathbb{F}_h$: finite field
- $\mathbb{F}_q$: *extension field* of $\mathbb{F}_h$ of degree ℓ, i.e. $q = h^\ell$
- $\mathbb{F}_{q^m}$: *extension field* of $\mathbb{F}_q$ of degree m
- $\boldsymbol{\beta} = (\beta_0, \beta_1, \ldots, \beta_{m-1})$: An *ordered basis* of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$
- Any element a from $\mathbb{F}_{q^m}$ can be represented w.r.t $\boldsymbol{\beta}$ by a *coordinate vector* $\underline{a} = \begin{pmatrix} a^{(0)} & \ldots & a^{(m-1)} \end{pmatrix}$ over $\mathbb{F}_q$ s.th.

$$a = \sum_{i=0}^{m-1} a^{(i)} \beta_i.$$

- *h-linearized polynomial*: $p(x) \stackrel{\text{def}}{=} \sum_{i=0}^{d} p_i x^{[i]}$ where $[i] \stackrel{\text{def}}{=} h^i$
- *h-degree*: $\deg_h(p(x)) \stackrel{\text{def}}{=} \max_i \{p_i \neq 0\}$

Some Definitions

- $\mathbb{L}_{q^m}[x]$: ring of h-linearized polynomials with coefficients from $\mathbb{F}_{q^m}$
- $\mathbb{L}_{q^m}[x]_{<k}$: set of all polynomials in $\mathbb{L}_{q^m}[x]$ with *h-degree less than k*
- For any $b \in \mathbb{F}_q$ and integer i we have: $b^{q^i} = b$
- Projective space $\mathcal{P}_h(N)$: set of all subspaces of $\mathbb{F}_h^N$
- Grassmannian $\mathcal{G}_h(N, n)$: set of all subspaces of $\mathcal{P}_h(N)$ of dimension n

The Operator Channel

$$\xrightarrow{\mathcal{V}} \boxed{\mathcal{H}_{n_t-\delta}(\mathcal{V}) \oplus \mathcal{E}} \xrightarrow{\mathcal{U}}$$

- *Input:* n_t-dimensional subspace $\mathcal{V} \in \mathcal{G}_h(N, n_t)$
- $\mathcal{H}_{n_t-\delta}(\mathcal{V})$ returns a random $(n_t - \delta)$-dimensional subspace of $\mathcal{V}$
  $\Rightarrow$ δ *deletions*
- γ-dimensional error space $\mathcal{E}$ with $\mathcal{V} \cap \mathcal{E} = \{\mathbf{0}\}$
  $\Rightarrow$ γ *insertions*
- *Output:* $(n_r = n_t - \delta + \gamma)$-dimensional subspace $\mathcal{U} \in \mathcal{G}_h(N, n_r)$

Definition

The subspace distance between $\mathcal{U}$ and $\mathcal{U}'$ is defined as

$$\begin{aligned} d_s(\mathcal{U},\mathcal{U}') &= \dim(\mathcal{U} \oplus \mathcal{U}') - \dim(\mathcal{U} \cap \mathcal{U}') \\ &= \dim(\mathcal{U}) + \dim(\mathcal{U}') - 2\dim(\mathcal{U} \cap \mathcal{U}') \end{aligned}$$

Properly Punctured Subspace (PSub) Codes

Definition (Properly Punctured Subspace Code)

Let $\boldsymbol{\alpha} = (\alpha_0\ \alpha_1\ \ldots \alpha_{n_t-1})^T \in \mathbb{F}_q^{n_t}$ be a vector containing $\mathbb{F}_h$-linearly independent code locators from $\mathbb{F}_q$. For $k \leq n_t$, a proper punctured subspace code $\mathrm{PSub}[\boldsymbol{\alpha}; n_t, k]$ of dimension n_t is defined as

$$\left\{ \langle(\boldsymbol{\alpha}\ f(\boldsymbol{\alpha}))\rangle_h \overset{\text{def}}{=} \left\langle \begin{pmatrix} \alpha_0 & f(\alpha_0) \\ \vdots & \vdots \\ \alpha_{n_t-1} & f(\alpha_{n_t-1}) \end{pmatrix} \right\rangle_h : f(x) \in \mathbb{L}_{q^m}[x]_{<k} \right\}. \quad (1)$$

- Subspace distance $d_s(\mathrm{PSub}[\boldsymbol{\alpha}; n_t, k]) = 2\,(n_t - k + 1)$
- Dimension of vector space: $N = \ell(1+m)$ over $\mathbb{F}_h$
- Unique decoding up to $d_s/2$ [1]: $\gamma + \delta \leq n_t - k$

How to decode beyond $d_s/2$?

[1] R. Kötter, F. R. Kschischang "Coding for Errors and Erasures in Random Linear Network Coding", 2008

Interleaved Subspace Codes [2]

Definition (m-Interleaved Subspace Code)

Let $\boldsymbol{\alpha} = (\alpha_0 \; \alpha_1 \; \ldots \alpha_{n_t-1})^T$ be a vector containing $\mathbb{F}_h$-linearly independent code locators from $\mathbb{F}_q$. For a fixed integer $k \leq n_t$, an interleaved subspace code $\mathrm{ISub}[m, \boldsymbol{\alpha}; n_t, k]$ of dimension n_t and interleaving order m is defined as

$$\left\{ \left\langle \left(\boldsymbol{\alpha} \; f^{(1)}(\boldsymbol{\alpha}) \; f^{(2)}(\boldsymbol{\alpha}) \; \ldots \; f^{(m)}(\boldsymbol{\alpha}) \right) \right\rangle_h : f^{(j)}(x) \in \mathbb{L}_q[x]_{<k}, \forall j \in [1, m] \right\}.$$

- Subspace distance $d_s(\mathrm{PSub}[\boldsymbol{\alpha}; n_t, k]) = 2\,(n_t - k + 1)$
- Dimension of vector space: $N = \ell(1 + m)$ over $\mathbb{F}_h$
- Decoding region [2]: $\frac{\gamma}{m} + \delta \leq (n_t - k)$
- Decoding failure probability (unique decoder): $< \frac{1}{q}$

[2] H. Bartz, A. Wacher-Zeh "Efficient Interpolation-Based Decoding of Interleaved Subspace and Gabidulin Codes", 2014

List Decoding of Interleaved Subspace Codes [2]

Interpolation Problem

Let

$$\mathcal{B}_{\mathcal{U}} = \left\{ \left(x_0, y_0^{(0)}, \dots, y_0^{(m-1)}\right), \dots, \left(x_{m-1}, y_{n_r-1}^{(0)}, \dots, y_{n_r-1}^{(m-1)}\right) \right\}$$

be a basis for the received subspace $\mathcal{U}$. Construct an $(m+1)$-variate h-linearized polynomial of the form

$$Q(x, y^{(0)}, \dots, y^{(m-1)}) = Q_0(x) + Q_1(y^{(0)}) + \dots + Q_m(y^{(m-1)})$$

that fulfills

- $Q(x_i, y_i^{(0)}, \dots, y_i^{(m-1)}) = 0, \quad \forall (x_i, y_i^{(0)}, \dots, y_i^{(m-1)}) \in \mathcal{B}_{\mathcal{U}}$
- $\deg_h(Q_0(x)) < D$
- $\deg_h(Q_j(x)) < D - (k-1), \forall j \in [1, m]$.

[2] H. Bartz, A. Wacher-Zeh "Efficient Interpolation-Based Decoding of Interleaved Subspace and Gabidulin Codes", 2014

List Decoding of Interleaved Subspace Codes [2]

Root-Finding Step

- If the number of insertions γ and deletions δ satisfy

$$\gamma + m\delta \leq m(n_t - k) \quad (2)$$

then

$$Q_0(x) + Q_1(f^{(0)}(x)) + \cdots + Q_m(f^{(m-1)}(x)) = 0. \quad (3)$$

- Find the list $\mathcal{L}_I$ of all $f^{(0)}(x), \ldots, f^{(m-1)}(x) \in \mathbb{L}_q[x]_{<k}$ of degree less than k that satisfy (3)
- The maximum list size is upper bounded by $|\mathcal{L}_I| \leq q^{k(m-1)}$
- Decoding failure probability (unique decoder): $< \frac{1}{q}$

[2] H. Bartz, A. Wacher-Zeh "Efficient Interpolation-Based Decoding of Interleaved Subspace and Gabidulin Codes", 2014

Power Decoding of Punctured Subspace Codes [3]

- Define $f^q(x) = \sum_{i=0}^{k-1} f_i^q x^{[i]}$
- For any $\alpha \in \mathbb{F}_q$ we have $(f(\alpha))^q = f^q(\alpha)$
- For $1 \leq s \leq m$ we can virtually extend each codeword of $\mathrm{PSub}[\boldsymbol{\alpha}; n, k]$ as

$$\left\langle \begin{pmatrix} \alpha_0 & f(\alpha_0) & f^q(\alpha_0) & \dots & f^{q^{s-1}}(\alpha_0) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{n_t-1} & f(\alpha_{n_t-1}) & f^q(\alpha_{n_t-1}) & \dots & f^{q^{s-1}}(\alpha_{n_t-1}) \end{pmatrix} \right\rangle_h$$

- The resulting codeword is a codeword of an s-interleaved code over $\mathbb{F}_{q^m}$ with correlated message polynomials $f(x), f^q(x), \dots, f^{q^{s-1}}(x)$
- The *virtually created symbols* do not need to be transmitted since they can be obtained at the receiver

[3] V. Guruswami and C. Xing, "List Decoding RS, Algebraic-Geometric, and Gabidulin Subcodes up to the Singleton Bound", 2012

Power Decoding of Punctured Subspace Codes [3]

- Define $f^q(x) = \sum_{i=0}^{k-1} f_i^q x^{[i]}$
- For any $\alpha \in \mathbb{F}_q$ we have $(f(\alpha))^q = f^q(\alpha)$
- For $1 \leq s \leq m$ we can virtually extend each codeword of $\mathrm{PSub}[\boldsymbol{\alpha}; n, k]$ as

$$\left\langle \begin{pmatrix} \alpha_0 & f(\alpha_0) & f^q(\alpha_0) & \dots & f^{q^{s-1}}(\alpha_0) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{n_t-1} & f(\alpha_{n_t-1}) & f^q(\alpha_{n_t-1}) & \dots & f^{q^{s-1}}(\alpha_{n_t-1}) \end{pmatrix} \right\rangle_h$$

- The resulting codeword is a codeword of an s-interleaved code over $\mathbb{F}_{q^m}$ with correlated message polynomials $f(x), f^q(x), \dots, f^{q^{s-1}}(x)$
- The *virtually created symbols* do not need to be transmitted since they can be obtained at the receiver

[3] V. Guruswami and C. Xing, "List Decoding RS, Algebraic-Geometric, and Gabidulin Subcodes up to the Singleton Bound", 2012

Power Decoding of Punctured Subspace Codes [3]

- Define $f^q(x) = \sum_{i=0}^{k-1} f_i^q x^{[i]}$
- For any $\alpha \in \mathbb{F}_q$ we have $(f(\alpha))^q = f^q(\alpha)$
- For $1 \leq s \leq m$ we can virtually extend each codeword of $\mathrm{PSub}[\boldsymbol{\alpha}; n, k]$ as

$$\left\langle \begin{pmatrix} \alpha_0 & f(\alpha_0) & f^q(\alpha_0) & \dots & f^{q^{s-1}}(\alpha_0) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{n_t-1} & f(\alpha_{n_t-1}) & f^q(\alpha_{n_t-1}) & \dots & f^{q^{s-1}}(\alpha_{n_t-1}) \end{pmatrix} \right\rangle_h$$

- The resulting codeword is a codeword of an s-interleaved code over $\mathbb{F}_{q^m}$ with correlated message polynomials $f(x), f^q(x), \dots, f^{q^{s-1}}(x)$
- The *virtually created symbols* do not need to be transmitted since they can be obtained at the receiver

[3] **V. Guruswami and C. Xing, "List Decoding RS, Algebraic-Geometric, and Gabidulin Subcodes up to the Singleton Bound", 2012**

Power Decoding of Punctured Subspace Codes [3]

- Define $f^q(x) = \sum_{i=0}^{k-1} f_i^q x^{[i]}$
- For any $\alpha \in \mathbb{F}_q$ we have $(f(\alpha))^q = f^q(\alpha)$
- For $1 \leq s \leq m$ we can virtually extend each codeword of $\mathrm{PSub}[\boldsymbol{\alpha}; n, k]$ as

$$\left\langle \begin{pmatrix} \alpha_0 & f(\alpha_0) & f^q(\alpha_0) & \dots & f^{q^{s-1}}(\alpha_0) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{n_t-1} & f(\alpha_{n_t-1}) & f^q(\alpha_{n_t-1}) & \dots & f^{q^{s-1}}(\alpha_{n_t-1}) \end{pmatrix} \right\rangle_h$$

- The resulting codeword is a codeword of an s-interleaved code over $\mathbb{F}_{q^m}$ with correlated message polynomials $f(x), f^q(x), \dots, f^{q^{s-1}}(x)$
- The *virtually created symbols* do not need to be transmitted since they can be obtained at the receiver

[3] **V. Guruswami and C. Xing, "List Decoding RS, Algebraic-Geometric, and Gabidulin Subcodes up to the Singleton Bound", 2012**

Power Decoding of Punctured Subspace Codes [3]

- Define $f^q(x) = \sum_{i=0}^{k-1} f_i^q x^{[i]}$
- For any $\alpha \in \mathbb{F}_q$ we have $(f(\alpha))^q = f^q(\alpha)$
- For $1 \leq s \leq m$ we can virtually extend each codeword of $\mathrm{PSub}[\boldsymbol{\alpha}; n, k]$ as

$$\left\langle \begin{pmatrix} \alpha_0 & f(\alpha_0) & f^q(\alpha_0) & \dots & f^{q^{s-1}}(\alpha_0) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{n_t-1} & f(\alpha_{n_t-1}) & f^q(\alpha_{n_t-1}) & \dots & f^{q^{s-1}}(\alpha_{n_t-1}) \end{pmatrix} \right\rangle_h$$

- The resulting codeword is a codeword of an s-interleaved code over $\mathbb{F}_{q^m}$ with correlated message polynomials $f(x), f^q(x), \dots, f^{q^{s-1}}(x)$
- The *virtually created symbols* do not need to be transmitted since they can be obtained at the receiver

[3] V. Guruswami and C. Xing, "List Decoding RS, Algebraic-Geometric, and Gabidulin Subcodes up to the Singleton Bound", 2012

Power Decoding of Punctured Subspace Codes

Interpolation Problem

Let

$$\mathcal{B}_{\mathcal{U}} = \left\{ \left(x_0, y_0\right), \dots, \left(x_{n_r-1}, y_{n_r-1}\right) \right\}$$

be a basis for the received subspace $\mathcal{U}$. Virtually create an s-interleaved received word with basis

$$\tilde{\mathcal{B}}_{\mathcal{U}} = \left\{ \left(x_0, y_0, y_0^q, \dots, y_0^{q^{s-1}}\right), \dots, \left(x_{n_r-1}, y_{n_r-1}, y_{n_r-1}^q, \dots, y_{n_r-1}^{q^{s-1}}\right) \right\}.$$

Construct a $(s+1)$-variate h-linearized polynomial of the form

$$Q(x, y, y^q, \dots, y^{q^{s-1}}) = Q_0(x) + Q_1(y) + Q_1(y^q) \cdots + Q_s(y^{q^{s-1}})$$

that fulfills

- $Q(x_i, y_i, y_i^q, \dots, y_i^{q^{s-1}}) = 0, \quad \forall (x_i, y_i, y_i^q, \dots, y_i^{q^{s-1}}) \in \tilde{\mathcal{B}}_{\mathcal{U}}$
- $\deg_h(Q_0(x)) < D$
- $\deg_h(Q_j(x)) < D - (k-1), \forall j \in [1, s]$.

Power Decoding of Punctured Subspace Codes

Interpolation Problem

Let

$$\mathcal{B}_{\mathcal{U}} = \left\{ (x_0, y_0), \ldots, (x_{n_r-1}, y_{n_r-1}) \right\}$$

be a basis for the received subspace $\mathcal{U}$. Virtually create an s-interleaved received word with basis

$$\tilde{\mathcal{B}}_{\mathcal{U}} = \left\{ (x_0, y_0, y_0^{q}, \ldots, y_0^{q^{s-1}}), \ldots, (x_{n_r-1}, y_{n_r-1}, y_{n_r-1}^{q}, \ldots, y_{n_r-1}^{q^{s-1}}) \right\}.$$

Construct a bivariate h-linearized polynomial of the form

$$Q(x, y) = Q_0(x) + Q_1(y) + Q_1(y^q) \cdots + Q_s(y^{q^{s-1}})$$

that fulfills

- $Q(x_i, y_i) = 0, \quad \forall (x_i, y_i) \in \mathcal{B}_{\mathcal{U}}$
- $\deg_h(Q_0(x)) < D$
- $\deg_h(Q_j(x)) < D - (k-1), \forall j \in [1, s]$.

Multivariate List Decoding

Root-Finding Step

- If the number of insertions γ and deletions δ satisfy

$$\gamma + s\delta \leq s\,(n_t - k) \tag{4}$$

then

$$Q_0(x) + Q_1(f(x)) + Q_2(f^{q}(x)) + \cdots + Q_s(f^{q^{s-1}}(x)) = 0. \tag{5}$$

- Find the list $\mathcal{L}_V$ of all $f(x)$ of degree less than k that satisfy (5)
- The maximum list size is upper bounded by $|\mathcal{L}_V| \leq q^{k(s-1)}$
- Decoding failure probability (unique decoder): $< \frac{1}{q}$

Comparison of Interleaved vs. Power Decoding

	Interleaved [2]	Power Decoding [3]
Interleaving order	m	$1 \leq s \leq m$
Decoding region	$\gamma + m\delta \leq m(n_t - k)$	$\gamma + s\delta \leq s(n_t - k)$
Worst-case list size	$q^{k(m-1)}$	$q^{k(s-1)}$
Comp. complexity	$\mathcal{O}(m^2 n^2)$ in $\mathbb{F}_q$	$\mathcal{O}(s^2 n^2)$ in $\mathbb{F}_{q^m}$

Contributions [4]:

- A decoding parameter $1 \leq s \leq m$ for the interleaved decoder that allows to control the decoding radius vs. maximum list size tradeoff
- We showed that $|\mathcal{L}_I| \leq |\mathcal{L}_V|$ if we use a minimal Gröbner basis for the interleaved decoder

[2] H. Bartz, A. Wacher-Zeh "Efficient Interpolation-Based Decoding of Interleaved Subspace and Gabidulin Codes", 2014

[3] V. Guruswami and C. Xing, "List Decoding RS, Algebraic-Geometric, and Gabidulin Subcodes up to the Singleton Bound", 2012

[4] H. Bartz, V. Sidorenko "On List-Decoding Schemes for Punctured Reed-Solomon, Gabidulin and Subspace Codes", Redundancy 2016, St. Petersburg, 2016

Comparison of Interleaved vs. Power Decoding

	Interleaved [2]	Power Decoding [3]
Interleaving order	m	$1 \leq s \leq m$
Decoding region	$\gamma + s\delta \leq s(n_t - k)$	$\gamma + s\delta \leq s(n_t - k)$
Worst-case list size	$q^{k(s-1)}$	$q^{k(s-1)}$
Comp. complexity	$\mathcal{O}(m^2 n^2)$ in $\mathbb{F}_q$	$\mathcal{O}(s^2 n^2)$ in $\mathbb{F}_{q^m}$

Contributions [4]:

- A decoding parameter $1 \leq s \leq m$ for the interleaved decoder that allows to control the decoding radius vs. maximum list size tradeoff
- We showed that $|\mathcal{L}_I| \leq |\mathcal{L}_V|$ if we use a minimal Gröbner basis for the interleaved decoder

[2] H. Bartz, A. Wacher-Zeh "Efficient Interpolation-Based Decoding of Interleaved Subspace and Gabidulin Codes", 2014
[3] V. Guruswami and C. Xing, "List Decoding RS, Algebraic-Geometric, and Gabidulin Subcodes up to the Singleton Bound", 2012
[4] H. Bartz, V. Sidorenko "On List-Decoding Schemes for Punctured Reed-Solomon, Gabidulin and Subspace Codes", Redundancy 2016, St. Petersburg, 2016

Comparison of Interleaved vs. Power Decoding

	Interleaved [2]	Power Decoding [3]
Interleaving order	m	$1 \leq s \leq m$
Decoding region	$\gamma + s\delta \leq s(n_t - k)$	$\gamma + s\delta \leq s(n_t - k)$
Worst-case list size	$q^{k(s-1)}$	$q^{k(s-1)}$
Comp. complexity	$\mathcal{O}(m^2 n^2)$ in $\mathbb{F}_q$	$\mathcal{O}(s^2 n^2)$ in $\mathbb{F}_{q^m}$

Contributions [4]:

- A decoding parameter $1 \leq s \leq m$ for the interleaved decoder that allows to control the decoding radius vs. maximum list size tradeoff
- We showed that $|\mathcal{L}_I| \leq |\mathcal{L}_V|$ if we use a minimal Gröbner basis for the interleaved decoder

[2] H. Bartz, A. Wacher-Zeh "Efficient Interpolation-Based Decoding of Interleaved Subspace and Gabidulin Codes", 2014

[3] V. Guruswami and C. Xing, "List Decoding RS, Algebraic-Geometric, and Gabidulin Subcodes up to the Singleton Bound", 2012

[4] H. Bartz, V. Sidorenko "On List-Decoding Schemes for Punctured Reed-Solomon, Gabidulin and Subspace Codes", Redundancy 2016, St. Petersburg, 2016

Conclusion

- *Analyzed* and *compared* power decoding for punctured subspace codes
- Proposed an efficient root-finding algorithm for the power decoder
- Showed equivalence of the interleaved decoder and the power decoder [4]
- Same results for Reed-Solomon and Gabidulin codes
- The equivalence was also established for syndrome-based decoding of Reed-Solomon an Gabidulin codes [5]
- Allows to choose the decoder with the *lower complexity*
  $\Rightarrow$ Decode punctured RS, Gabidulin and subspace codes as m-interleaved codes over the subfield $\mathbb{F}_q$

---

[4] H. Bartz, V. Sidorenko "On List-Decoding Schemes for Punctured Reed-Solomon, Gabidulin and Subspace Codes", XV International Symposium on Problems of Redundancy in Information and Control Systems, St. Petersburg, 20016

[5] H. Bartz, V. Sidorenko "On Syndrome Decoding of Punctured Reed-Solomon and Gabidulin Codes", ACCT 2016

Thank you! Questions?

{hannes.bartz, vladimir.sidorenko}@tum.de