

General Linearized Polynomial Interpolation and Its Applications

Hongmei Xie¹ Zhiyuan Yan¹ Bruce W. Suter²

¹Department of ECE, Lehigh University

²Air Force Research Laboratory

NetCod 2011, Tuesday July 26, 2011

Supported in part by NSF under Grant ECCS-1055877 and in part by a grant from Thales Communications, Inc.

Outline

Overview

Background

General Interpolation by Linearized Polynomials

Decoding of KK Codes

Decoding of MV Codes

References

www.leaderstudio.net

Interpolation

- Interpolation: construct new data points within the range of a discrete set of known data points
- Curve fitting: find a function that produce the data points
- Polynomial interpolation: sufficient for functions over finite fields

Interpolation in Classic Coding

bound	Singleton
optimal codes	Reed–Solomon
list decoding ($L = 1$)	Welch–Berlekamp
GMD	Kötter
list decoding ($L > 1$)	Guruswami–Sudan

Interpolation in Network Coding Error Control

bound	Singleton	Singleton	
(quasi)optimal codes	Gabidulin	Kötter–Kschischang	
other codes			Mahdavifar–Vardy
list decoding ($L = 1$)	Loidreau	Kötter–Kschischang	
list decoding ($L > 1$)			Mahdavifar–Vardy

Interpolation over Free Modules

- Extension of Kötter interpolation by Wang–McEliece–Watanabe [WMW05]
- Propose an interpolation algorithm for interpolation over free modules of polynomial rings
- Special cases of interpolation algorithm:
 - Kötter interpolation algorithm
 - Welch–Berlekamp algorithm

Main Results

- Parallel the work by Wang–McEliece–Watanabe
- Propose an interpolation algorithm for interpolation over free modules of *linearized* polynomial rings
- Special cases of interpolation algorithm:
 - Loidreau's algorithm
 - Kötter–Kschischang algorithm
 - MahdaviFar–Vardy algorithm
- Interpolation algorithm also has reduced complexities

Linearized Polynomial Ring

- A *linearized polynomial* [Ore33] over \mathbb{F}_{q^m}

$$l(x) = \sum_{i=0}^n a_i x^{[i]}, \quad [i] = q^i, a_i \in \mathbb{F}_{q^m}$$

- *q-degree*: $\deg_q(l(x)) = \max_{a_i \neq 0} \{i\}$
- $L[x] = \{\text{all linearized polynomials over } \mathbb{F}_{q^m}\}$: a ring
 $l_1(x), l_2(x) \in L[x], \alpha, \beta \in \mathbb{F}_{q^m}$
 - $\alpha l_1(x) + \beta l_2(x) \in L[x]$
 - $l_1(x) \otimes l_2(x) \stackrel{\text{def}}{=} l_1(l_2(x)) \in L[x]$

Subspace Codes

- RLNC Noncoherent error control for RLNC
- W : a vector space over \mathbb{F}_q
 $\mathcal{P}(W)$: set of all subspaces of W
- *Subspace distance*: metric on $\mathcal{P}(W)$ [KK08]
 $d_s(V, U) \stackrel{\text{def}}{=} \dim(V + U) - \dim(V \cap U)$
- *Subspace code*: a subset of $\mathcal{P}(W)$
 - Kötter–Kschischang (KK) codes
 - MahdaviFar–Vardy (MV) codes

KK Codes

- $\alpha_1, \alpha_2, \dots, \alpha_l \in \mathbb{F}_{q^m}$, linearly independent
- Message: $\mathbf{u} = (u_0, u_1, \dots, u_{k-1}) \in \mathbb{F}_{q^m}^k \Leftrightarrow u(x) = \sum_{i=0}^{k-1} u_i x^i$
 Codeword: $V = \langle (\alpha_1, u(\alpha_1)), (\alpha_2, u(\alpha_2)), \dots, (\alpha_l, u(\alpha_l)) \rangle$
 - $W = \langle \alpha_1, \alpha_2, \dots, \alpha_l \rangle \oplus \mathbb{F}_{q^m}$, $\dim(W) = l + m$
- Transmit $V \in \mathcal{P}(W)$, $\dim(V) = l$
- $\dim(\text{error}) = t$, $\dim(\text{erasure}) = \rho$
 \Rightarrow Receive $U \in \mathcal{P}(W)$, $\dim(U) = l - \rho + t = r$
- Recover V uniquely from U if $\rho + t < l - k + 1$ [KK08]

Sudan Style List-1 Decoding Algorithm for KK Codes

- Find $\{(x_1, y_1), (x_2, y_2), \dots, (x_r, y_r)\}$, a basis for U
- *Interpolation*: find nonzero bivariate linearized polynomial $Q(x, y) = Q_x(x) + Q_y(y)$ s.t.
 - $Q(x_i, y_i) = 0, \quad i = 1, 2, \dots, r$
 - $Q_x(x), Q_y(x) \in L[x]$
 - $\deg_q(Q_x(x)) \leq \tau - 1, \deg_q(Q_y(y)) \leq \tau - k$
- *Factorization*: find $\hat{u}(x)$ from $Q(x, \hat{u}(x)) \equiv 0$
- List size is one \Rightarrow bounded distance decoder

Kötter–Kschischang Interpolation

- *Initialization:* $f_0^{(0)}(x, y) = x$, $f_1^{(0)}(x, y) = y$
- *Recursion:* $f_j^{(i-1)}(x, y) \Rightarrow f_j^{(i)}(x, y)$, $i = 1, 2, \dots, r, j = 0, 1$
 - $f_0^{(i)}(x, y)$ interpolates through the first i points, x -minimal
 - $f_1^{(i)}(x, y)$ interpolates through the first i points, y -minimal
 - $f_j^{(i)}(x, y)$ updated based on discrepancies
- *Output:* $f_0^{(r)}(x, y)$ or $f_1^{(r)}(x, y)$, whichever of a smaller order
- Decodability guaranteed if selecting $\tau = \lceil (r + k)/2 \rceil$ [KK08]

l -dimensional MV Codes

- $\alpha_1, \alpha_2, \dots, \alpha_l \in \mathbb{F}_{q^{ml}}$, linearly independent
- \mathcal{L} : decoding list, $|\mathcal{L}| \leq L$
- Message: $\mathbf{u} = (u_0, u_1, \dots, u_{k-1}) \in \mathbb{F}_q^k \Leftrightarrow u(x) = \sum_{i=0}^{k-1} u_i x^i$
 Codeword: $V = \langle \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_l \rangle$
 - $\mathbf{v}_1 = (\alpha_1, u(\alpha_1), u^{\otimes 2}(\alpha_1), \dots, u^{\otimes L}(\alpha_1))$
 - $\mathbf{v}_i = (\alpha_i, \frac{u(\alpha_i)}{\alpha_i}, \dots, \frac{u^{\otimes L}(\alpha_i)}{\alpha_i})$, $i = 2, 3, \dots, l$
 - $W = \langle \alpha_1, \alpha_2, \dots, \alpha_l \rangle \oplus \underbrace{\mathbb{F}_{q^m} \oplus \dots \oplus \mathbb{F}_{q^m}}_{L \text{ times}}$
- $V \in \mathcal{P}(W)$, $\dim(V) = l$
- $\dim(\text{error}) = t$
 \Rightarrow Received: $U \in W$, $\dim(U) = l + t$
- $V \in \mathcal{L}$ if $t < lL - L(L+1)\frac{k-1}{2m}$

List Decoding of MV Codes

- Find $(\beta_{j,0}, \beta_{j,1}, \dots, \beta_{j,L})$ to be interpolated [MV10]
 - $j = 1, 2, \dots, N_p, \quad N_p \leq (t + l)m$
- *Interpolation*: find nonzero multivariate linearized polynomial $Q(y_0, y_1, y_2, \dots, y_L) = \sum_{i=0}^L Q_i(y_i)$ s.t.
 - $Q(\beta_{j,0}, \beta_{j,1}, \dots, \beta_{j,L}) = 0$
 - $Q_i(y_i) \in L[y_i], \deg_q(Q_i(y_i)) \leq ml - i(k - 1) - 1$
- *Factorization*: find $\hat{u}(x)$ s.t. $Q(x, \hat{u}(x), \hat{u}^{\otimes 2}(x), \dots, \hat{u}^{\otimes L}(x)) \equiv 0$

Key Ideas

- Free module V of linearized polynomial ring
→ also a vector space
- Need a polynomial with a smaller “degree”
→ total ordering on V
- Treat constraints as linear functionals K_i 's
→ find the “smallest” in the intersection of the kernels $\cap K_i$
- Solve it by Berlekamp's iterative-discrepancy idea

Free $L[x]$ -module

- $L[x]$ over \mathbb{F}_{q^m} : linearized polynomial ring
- $\left\{ \begin{array}{l} \text{Basis: } B = \{b_0, b_1, \dots, b_L\} \\ \text{Multiplication: } \circ \end{array} \right\} \Rightarrow V$: free $L[x]$ -module
 $\Rightarrow Q = \sum_{j=0}^L l_j(x) \circ b_j = \sum_{i,j} \sum_{i \geq 0} a_{i,j} x^{[i]} \circ b_j \in V$
- V : a vector space over \mathbb{F}_{q^m} with basis
 $M = \{x^{[i]} \circ b_j, i \geq 0, j = 0, 1, \dots, L\} = \{\phi_s\}_{s \geq 0}$
- Total ordering on M : $\phi_s < \phi_t$ if $s < t$
- $Q = \sum_{i=0}^S a_i \phi_i, a_S \neq 0$.
 - $\text{order}(Q) = S$, order of Q
 - $\text{LM}(Q) = \phi_S$, leading monomial

General Interpolation Problem

- Linear functionals $D_i: V \rightarrow \mathbb{F}_{q^m}$, $i = 1, 2, \dots, C$
Kernels $K_i \Rightarrow \bar{K}_i = K_1 \cap K_2 \cap \dots \cap K_i$, $L[x]$ -submodule
- $\text{order}(Q)$ lowest in $\bar{K}_i \Rightarrow Q$ is a *minimum* in \bar{K}_i
- General interpolation problem: find a minimum $Q^* \in \bar{K}_C$

General Interpolation Algorithm

Algorithm 1 General Interpolation by Linearized Polynomials

```

for  $j = 0$  to  $L$  do
     $g_{0,j} \leftarrow b_j$ 
for  $i = 0$  to  $C - 1$  do
    for  $j = 0$  to  $L$  do
         $g_{i+1,j} \leftarrow g_{i,j}$ 
         $\Delta_{i+1,j} \leftarrow D_{i+1}(g_{i,j})$ 
         $J \leftarrow \{j : \Delta_{i+1,j} \neq 0\}$ 
        if  $J \neq \emptyset$  then
             $j^* \leftarrow \underset{j \in J}{\operatorname{argmin}} \{g_{i,j}\}$ 
            for  $j \in J$  do
                if  $j \neq j^*$  then
                     $g_{i+1,j} \leftarrow \Delta_{i+1,j^*} g_{i,j} - \Delta_{i+1,j} g_{i,j^*}$ 
                else if  $j = j^*$  then
                     $g_{i+1,j} \leftarrow \Delta_{i+1,j}(x^{[1]} \circ g_{i,j}) - D_{i+1}(x^{[1]} \circ g_{i,j}) g_{i,j}$ 
     $Q^* \leftarrow \min_j g_{C,j}$ 

```

Complexity Analysis

In Algorithm 1:

- C : number of iterations
- $L + 1$: size of the basis of the free module
- D : highest q -degree of linearized polynomials

Overall complexity of Algorithm 1:

- $O(CDL^2)$ finite field additions
- $O(CDL^2)$ finite field multiplications
- $O(CL)$ linear functional calculations
- $O(C)$ multiplications between $L[x]$ and V

Decoding of KK Codes

A general interpolation problem.

- $$\left. \begin{aligned} B = \{b_0, b_1\} = \{x, y\} \\ l(x) \circ b_j \stackrel{\text{def}}{=} l(b_j), \quad j = 0, 1 \end{aligned} \right\} \Rightarrow Q = \sum_{i,j} a_{i,j} x^{[i]} \circ b_j \in V$$
- $(1, k-1)$ -weighted degree: $\deg_{1,k-1}(x^{[i]} \circ b_j) \stackrel{\text{def}}{=} i + j * (k-1)$
 \Rightarrow Total ordering: $x^{[i]} \circ b_j < x^{[i']} \circ b_{j'}$ if
 - $\deg_{1,k-1}(x^{[i]} \circ b_j) < \deg_{1,k-1}(x^{[i']} \circ b_{j'})$, or
 - $\deg_{1,k-1}(x^{[i]} \circ b_j) = \deg_{1,k-1}(x^{[i']} \circ b_{j'})$ and $j < j'$
- Linear functionals: $D_i(Q) = Q(x_i, y_i)$, evaluation of $Q(x, y)$ at (x_i, y_i)
 \Rightarrow Kernels: $K_i, \quad i = 1, 2, \dots, r$
- \overline{K}_i is an $L[x]$ -submodule

Decoding KK Codes by Algorithm 1

Algorithm 1 finds a **minimum** nonzero solution

- Initialization: $g_{0,0} = x, \quad g_{0,1} = y$
- Recursion operations
 - Multiplication: $l(x) \circ b_j \stackrel{\text{def}}{=} l(b_j)$
 - Update: $g_{i+1,j^*} = D_{i+1}(g_{i,j^*})(x^{[1]} \circ g_{i,j^*}) - D_{i+1}(x^{[1]} \circ g_{i,j^*})g_{i,j^*}$
 $\Rightarrow g_{i+1,j^*} = g_{i,j^*}^q - (D_{i+1}(g_{i,j^*}))^{q-1}g_{i,j^*}$ since $D_{i+1}(g_{i,j^*}) \neq 0$

Lemma

When $L = 1$, Algorithm 1 reduces to the Sudan-style list-1 decoding algorithm in [KK08]

Complexity of Decoding KK Codes

- $L = 1, C = r, D = \lfloor \frac{r+k}{2} \rfloor$
- Multiplication \circ : cyclic shift under normal basis [GY08]
- Linear functional:
 - $O(DL)$ finite field multiplications
 - $O(DL)$ finite field additions
- Total complexity:
 - $O(r(r+k))$ finite field multiplications
 - $O(r(r+k))$ finite field additions






Decoding of MV Codes

Also a general interpolation problem

- $$\begin{cases} B = \{b_0, b_1, \dots, b_L\} = \{y_0, y_1, \dots, y_L\} \\ l(x) \circ b_j \stackrel{\text{def}}{=} l(b_j), \quad j = 0, 1, \dots, L \end{cases}$$
- $\Rightarrow Q = \sum_{i,j} x^{[i]} \circ b_j \in V$
- Total ordering, linear functionals *etc.* : as KK codes
- Algorithm 1 gives a **minimum** nonzero solution
 - $g_{0,j} = b_j, \quad j = 0, 1, \dots, L$
 - $l(x) \circ b_j \stackrel{\text{def}}{=} l(b_j), \quad j = 0, 1, \dots, L$

Complexity of Decoding MV Codes

- By Gaussian elimination: $O(L^2 m^2 (t + l)^2 (k - 1))$
- By Algorithm 1: $O(L^2 m^2 (t + l) l)$
 - $C = (t + l)m$
 - $D = ml - 1$
- Algorithm 1 has a lower complexity than Gaussian elimination

-  Maximilien Gadouleau and Zhiyuan Yan.
Complexity of decoding Gabidulin codes.
In 42nd Annual Conference on Information Sciences and Systems, pages 1081–1085, Princeton, USA, March 2008.
-  Ralf Kötter and Frank R. Kschischang.
Coding for errors and erasures in random network coding.
IEEE Trans. Info. Theory, 54(8):3579–3591, August 2008.
-  H. Mahdaviifar and A. Vardy.
Algebraic list-decoding on the operator channel.
In Proc. IEEE Int. Symp. Info. Theory, pages 1193–1197, Austin, USA, June 2010.
-  Ö. Ore.
On a special class of polynomials.
Transactions of the American Mathematical Society, 35:559–584, 1933.
-  B. Wang, R. J. McEliece, and K. Watanabe.
Kötter interpolation over free modules.

In Proc. 2005 Allerton Conf. Communications Control and Computing, pages 2197–2206, Monticello, IL, October 2005.

www.leaderstudio.net