Polynomial interpolation over finite fields and applications to list decoding of Reed-Solomon codes

Roberta Barbi

December 17, 2015

Codes

Let $\mathbb{F}_q$ be a finite field, with $q = p^m$ for $m \in \mathbb{N}$ and p a prime number.

(Linear) Code

Let $k, n \in \mathbb{N}$ be such that $1 \leq k \leq n$. A code is any non-empty subset of $(\mathbb{F}_q)^n$.
A **linear code** $\mathscr{C}$ is a k-dimensional vector subspace of $(\mathbb{F}_q)^n$. We say that $\mathscr{C}$ is a linear code over $\mathbb{F}_q$ with *length* n and *dimension* k and we write $[n, k]_q$.

Codes

Let $\mathbb{F}_q$ be a finite field, with $q = p^m$ for $m \in \mathbb{N}$ and p a prime number.

(Linear) Code

Let $k, n \in \mathbb{N}$ be such that $1 \leq k \leq n$. A code is any non-empty subset of $(\mathbb{F}_q)^n$.
A **linear code** $\mathscr{C}$ is a k-dimensional vector subspace of $(\mathbb{F}_q)^n$. We say that $\mathscr{C}$ is a linear code over $\mathbb{F}_q$ with *length* n and *dimension* k and we write $[n, k]_q$.

Distance of a code

The *distance* of the code $\mathscr{C}$ is the minimum distance between codewords of $\mathscr{C}$.
The distance between two codewords is the number of coordinates in which these two codewords differ.

Codes

Let $\mathbb{F}_q$ be a finite field, with $q = p^m$ for $m \in \mathbb{N}$ and p a prime number.

(Linear) Code

Let $k, n \in \mathbb{N}$ be such that $1 \leq k \leq n$. A code is any non-empty subset of $(\mathbb{F}_q)^n$.
A **linear code** $\mathscr{C}$ is a k-dimensional vector subspace of $(\mathbb{F}_q)^n$. We say that $\mathscr{C}$ is a linear code over $\mathbb{F}_q$ with *length* n and *dimension* k and we write $[n, k]_q$.

Distance of a code

The *distance* of the code $\mathscr{C}$ is the minimum distance between codewords of $\mathscr{C}$.
The distance between two codewords is the number of coordinates in which these two codewords differ.

Reed-Solomon code

Let $\mathbb{F}_q$ be a finite field. Set $n = q - 1$ and $\mathbb{F}_q^* = \{\alpha_1, \ldots, \alpha_n\}$. Define the Reed-Solomon code over $\mathbb{F}_q$ of length n and dimension $1 \leq k \leq n$:

$$RS_{n,k} = \Big\{ \big(f(\alpha_1), \ldots, f(\alpha_n)\big) \ : \ f \in \mathbb{F}_q[x], \ \deg(f) \leq k - 1 \Big\} \tag{1}$$

Then $d(RS_{n,k}) = n - k + 1$.

List decoding problem

Correction capability

The correction capability of a $[n, k, d]_q$ code $\mathscr{C}$ is $\tau = \lfloor \frac{d-1}{2} \rfloor$.

On good channels, that is channels introducing few noise, one assumes that at most τ errors happened.
What if we have a noisy channel and we want to assume that more than τ errors may happen?

List decoding problem

Correction capability

The correction capability of a $[n, k, d]_q$ code $\mathscr{C}$ is $\tau = \lfloor \frac{d-1}{2} \rfloor$.

On good channels, that is channels introducing few noise, one assumes that at most τ errors happened.
What if we have a noisy channel and we want to assume that more than τ errors may happen?

The setting

- Let $RS_{n,k}$ be the Reed-Solomon code over $\mathbb{F}_q$ with length $n = q - 1$ and dimension $1 \leq k \leq n$.
- Let $\{\alpha_1, \ldots, \alpha_n\} = \mathbb{F}_q^*$ be the non-zero elements of the field $\mathbb{F}_q$.
- Let $v = (v_1, \ldots, v_n)$ be the received vector.
- Let $\underline{\mathcal{A} = \{ (\alpha_1, v_1), \ldots, (\alpha_n, v_n) \}} \subseteq (\mathbb{F}_q)^2$.

List decoding of Reed-Solomon codes

List decoding of $RS_{n,k}$

Find a list of all functions $f : \mathbb{F}_q \to \mathbb{F}_q$ such that $f(x)$ is a polynomial of degree at most $k-1$ with

$$\left| \left\{ i \in \{1, \ldots, n\} \ : \ f(\alpha_i) \neq v_i \right\} \right| \leq \mathrm{e}$$

where e is the number of errors that may happen.

Sudan list decoding

Let $m = x^\alpha y^\beta$. Define $\mathrm{w}_{k-1}(m) = \alpha + (k-1)\beta$.

Sudan list decoding

Find any function $Q(x, y) : (\mathbb{F}_q)^2 \to \mathbb{F}_q$ not identically zero satisfying

- an interpolation condition: $Q(\alpha_i, v_i) = 0, \quad \forall 1 \le i \le n$
- a degree constraint: $\mathrm{w}_{k-1}(Q(x, y)) \le m + l(k-1)$, certain $l, m \in \mathbb{N}$

Then factor $Q(x, y)$ and output all its factors of the form $y - g(x)$ with $\deg g(x) \le k - 1$.

Sudan list decoding

Let $m = x^\alpha y^\beta$. Define $\mathrm{w}_{k-1}(m) = \alpha + (k-1)\beta$.

Sudan list decoding

Find any function $Q(x,y) : (\mathbb{F}_q)^2 \to \mathbb{F}_q$ not identically zero satisfying

- an interpolation condition: $Q(\alpha_i, v_i) = 0, \quad \forall 1 \leq i \leq n$
- a degree constraint: $\mathrm{w}_{k-1}(Q(x,y)) \leq m + l(k-1)$, certain $l, m \in \mathbb{N}$

Then factor $Q(x,y)$ and output all its factors of the form $y - g(x)$ with $\deg g(x) \leq k-1$.

The interpolation condition

Polynomials in the vanishing ideal of $\mathcal{A}$, that is in $I(\mathcal{A})$, satisfy the interpolation condition:

$$I(\mathcal{A}) = I\Big(\left\{ (\alpha_1, v_1), \ldots, (\alpha_n, v_n) \right\}\Big)$$

Gröbner bases

Gröbner basis

Fix a monomial order $\prec$ over $\mathbb{K}[x_1, \ldots, x_n]$. Let $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be an ideal. A set $G \subset I$ such that $\langle G \rangle = I$ and $\mathrm{lm}(G) = \mathrm{lm}(I)$ is said to be a Gröbner basis (GB) for the ideal I.

Gröbner bases

Gröbner basis

Fix a monomial order $\prec$ over $\mathbb{K}[x_1, \ldots, x_n]$. Let $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be an ideal. A set $G \subset I$ such that $\langle G \rangle = I$ and $\mathrm{lm}(G) = \mathrm{lm}(I)$ is said to be a Gröbner basis (GB) for the ideal I.

Staircase

Fix a monomial order $\prec$ over $\mathbb{K}[x_1, \ldots, x_n]$. Let $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be an ideal. The set $N(I) = \mathcal{M} \setminus \mathrm{lm}(I)$ is called the Hilbert staircase or the footprint for I.

Gröbner bases

Gröbner basis

Fix a monomial order $\prec$ over $\mathbb{K}[x_1, \ldots, x_n]$. Let $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be an ideal. A set $G \subset I$ such that $\langle G \rangle = I$ and $\mathrm{lm}(G) = \mathrm{lm}(I)$ is said to be a Gröbner basis (GB) for the ideal I.

Staircase

Fix a monomial order $\prec$ over $\mathbb{K}[x_1, \ldots, x_n]$. Let $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be an ideal. The set $N(I) = \mathcal{M} \setminus \mathrm{lm}(I)$ is called the Hilbert staircase or the footprint for I.

Degree constraint

With the purpose of minimizing the weighted degree:

- The minimal polynomial wrt a monomial ordering is in a Gröbner basis wrt that ordering.
- So we compute a Gröbner basis and consider the polynomial having smallest weighted degree in it.

A Gröbner basis approach

The existence of $Q(x, y)$

Define $\mathrm{mult}_{(0,0)} f$ as the smallest $m \in \mathbb{N}$ such that a monomial of total degree m occurs in the polynomial f. Then $\mathrm{mult}_{(a,b)} f = \mathrm{mult}_{(0,0)} g$, where $g(x, y) = f(x + a, y + b)$.

Define $\text{mult}_{(0,0)} f$ as the smallest $m \in \mathbb{N}$ such that a monomial of total degree m occurs in the polynomial f. Then $\text{mult}_{(a,b)} f = \text{mult}_{(0,0)} g$, where $g(x, y) = f(x + a, y + b)$.

The ideal of points in $\mathcal{A}$ with multiplicity r

$$\begin{aligned} I_{v,\mathrm{r}} &= \{f \in \mathbb{F}_q[x, y] \ : \ \text{mult}_{(\alpha_i, v_i)}(f) \geq \mathrm{r} \text{ for } 1 \leq i \leq n\} \cup \{0\} \\ &= \left\langle (y - h_v)^i \left(\prod (x - \alpha_j) \right)^{\mathrm{r}-i} \ : \ 0 \leq i \leq \mathrm{r} \right\rangle \end{aligned} \tag{2}$$

A Gröbner basis approach

The existence of $Q(x, y)$

Define $\text{mult}_{(0,0)} f$ as the smallest $m \in \mathbb{N}$ such that a monomial of total degree m occurs in the polynomial f. Then $\text{mult}_{(a,b)} f = \text{mult}_{(0,0)} g$, where $g(x, y) = f(x + a, y + b)$.

The ideal of points in $\mathcal{A}$ with multiplicity r

$$\begin{aligned} I_{v,\mathrm{r}} &= \{f \in \mathbb{F}_q[x, y] \ : \ \text{mult}_{(\alpha_i, v_i)}(f) \geq \mathrm{r} \text{ for } 1 \leq i \leq n\} \cup \{0\} \\ &= \left\langle (y - h_v)^i \Big(\prod (x - \alpha_j) \Big)^{\mathrm{r}-i} \ : \ 0 \leq i \leq \mathrm{r} \right\rangle \end{aligned} \tag{2}$$

Proposition (Sudan list decoding)

Suppose that $f \in I_{v,\mathrm{r}}$ is non-zero. If $c \in RS_{n,k}$ satisfies:

$$d(v, c) < n - \frac{\mathrm{w}_{k-1}(f)}{\mathrm{r}} \tag{3}$$

then $h_c(x)$ is a root of f as a polynomial in y over $\mathbb{F}_q[x]$, that is $f(x, h_c(x)) = 0$.

Define $\text{mult}_{(0,0)} f$ as the smallest $m \in \mathbb{N}$ such that a monomial of total degree m occurs in the polynomial f. Then $\text{mult}_{(a,b)} f = \text{mult}_{(0,0)} g$, where $g(x, y) = f(x + a, y + b)$.

The ideal of points in $\mathcal{A}$ with multiplicity r

$$
\begin{aligned}
I_{v,\mathrm{r}} &= \{f \in \mathbb{F}_q[x, y] \ : \ \text{mult}_{(\alpha_i, v_i)}(f) \geq \mathrm{r} \text{ for } 1 \leq i \leq n\} \cup \{0\} \\
&= \left\langle (y - h_v)^i \left(\prod (x - \alpha_j) \right)^{\mathrm{r}-i} \ : \ 0 \leq i \leq \mathrm{r} \right\rangle
\end{aligned} \tag{2}
$$

Proposition (Sudan list decoding)

Suppose that $f \in I_{v,\mathrm{r}}$ is non-zero. If $c \in RS_{n,k}$ satisfies:

$$
d(v, c) < n - \frac{\mathrm{w}_{k-1}(f)}{\mathrm{r}} \tag{3}
$$

then $h_c(x)$ is a root of f as a polynomial in y over $\mathbb{F}_q[x]$, that is $f(x, h_c(x)) = 0$.

$\Rightarrow$ We may use the ideal $I_{v,\mathrm{r}}$ for list dec. if $\exists\, Q \in I_{v,\mathrm{r}}$ s.t. $\mathrm{w}_{k-1}(Q) < \mathrm{r}\big(n - d(v, c)\big)$.

$(1, k-1)$-weighted degree ordering $\prec_{\mathrm{w}_{k-1}}$

Let $m_1 = x^{i_1}y^{j_1}$ and $m_2 = x^{i_2}y^{j_2}$. Define $\mathrm{w}_{k-1}(m_1) = i_1 + j_1(k-1)$. Then $m_1 \prec_{\mathrm{w}_{k-1}} m_2$ if:

$$\begin{cases} \mathrm{w}_{k-1}(m_1) < \mathrm{w}_{k-1}(m_2) \text{ or} \\ \mathrm{w}_{k-1}(m_1) = \mathrm{w}_{k-1}(m_2) \text{ and } j_1 < j_2 \end{cases}$$

$(1, k-1)$-weighted degree ordering $\prec_{w_{k-1}}$

Let $m_1 = x^{i_1}y^{j_1}$ and $m_2 = x^{i_2}y^{j_2}$. Define $w_{k-1}(m_1) = i_1 + j_1(k-1)$. Then $m_1 \prec_{w_{k-1}} m_2$ if:

$$\begin{cases} w_{k-1}(m_1) < w_{k-1}(m_2) \text{ or} \\ w_{k-1}(m_1) = w_{k-1}(m_2) \text{ and } j_1 < j_2 \end{cases}$$

A Gröbner basis approach

1. We fix the multiplicity r (starting with $r = 1$).
2. As a candidate for $Q(x, y)$ we choose the minimal polynomial $\Psi(x, y)$ of $I_{v,r}$ wrt $(1, k-1)$-weighted degree ordering.
3. We find $\Psi(x, y)$ by computing a Gröbner basis of $I_{v,r}$ wrt $(1, k-1)$-weighted degree ordering.
   - $\rightarrow$ If $\Psi(x, y)$ satisfies (3) then we set $Q(x, y) = \Psi(x, y)$.
   - $\rightarrow$ If $\Psi(x, y)$ does not satisfy (3), meaning that its weighted degree is too large, we must increase r (go back to 1).

Buchberger-Möller algorithm over $\mathcal{A}$

Compute a Gröbner basis for $I(\mathcal{A})$ wrt lexicographical ordering $x \prec_{\text{lex}} y$ using Buchberger-Möller algorithm:

$$G^{(lex)} = \left\{ \prod_{i=1}^{n} (x - \alpha_i) \, , \; y - h_v(x) \right\}$$

where $h_v(x)$ is the Lagrange interpolant $h_v(\alpha_i) = v_i$: $h_v(x) = \sum_{i=1}^{n} v_i \prod_{\substack{j=1 \\ j \neq i}}^{n} \frac{x - \alpha_j}{\alpha_i - \alpha_j}$.

Buchberger-Möller algorithm over $\mathcal{A}$

Compute a Gröbner basis for $I(\mathcal{A})$ wrt lexicographical ordering $x \prec_{\text{lex}} y$ using Buchberger-Möller algorithm:

$$G^{(lex)} = \left\{ \prod_{i=1}^{n} (x - \alpha_i)\ ,\ y - h_v(x) \right\}$$

where $h_v(x)$ is the Lagrange interpolant $h_v(\alpha_i) = v_i$: $h_v(x) = \sum_{i=1}^{n} v_i \prod_{\substack{j=1 \\ j \neq i}}^{n} \frac{x - \alpha_j}{\alpha_i - \alpha_j}$.

$G^{(lex)}$ is not useful for list decoding:

- The only polynomial in y is $y - h_v(x)$.
- The interpolant $h_v(x)$ cannot represent a codeword (received vector is not a codeword).

Gröbner basis for $I(\mathcal{A})$ wrt $\prec_{\mathrm{w}_{k-1}}$: Buchberger-Möller algorithm

A GB wrt $(1, k-1)$-weighted degree ordering for the vanishing ideal $I(\mathcal{A}_k)$ where $\mathcal{A}_k = \{(\alpha_1, v_1), \ldots, (\alpha_k, v_k)\}$ is given by

$$G^{(k)} = \left\{ y - h_{(v_1, \ldots, v_k)}(x) \, , \, \prod_{i=1}^{k} (x - \alpha_i) \right\}$$

Gröbner basis for $I(\mathcal{A})$ wrt $\prec_{w_{k-1}}$: Buchberger-Möller algorithm

A GB wrt $(1, k-1)$-weighted degree ordering for the vanishing ideal $I(\mathcal{A}_k)$ where $\mathcal{A}_k = \{(\alpha_1, v_1), \ldots, (\alpha_k, v_k)\}$ is given by

$$G^{(k)} = \left\{ y - h_{(v_1, \ldots, v_k)}(x) \, , \, \prod_{i=1}^{k} (x - \alpha_i) \right\}$$

Complexity

Buchberger-Möller takes $O(N^3)$ where N is the number of points in input.
We use $G^{(k)}$ and $\mathcal{A}_k$ as input of Buchberger-Möller algorithm thus reducing the complexity to $O((n-k)^3)$:

Constraint over k	$k \geq n - \sqrt[3]{n}$	$k \geq n - \sqrt[3]{n^2}$
BM complexity	$(n-k)^3 \approx n$	$(n-k)^3 \approx n^2$
Interpolation complexity	k^2	k^2

Given $G^{(lex)}$ and $\prec_{w_{k-1}}$, FGLM algorithm computes a GB for $\langle G^{(lex)} \rangle$ wrt $\prec_{w_{k-1}}$ in time $O(n^3)$:

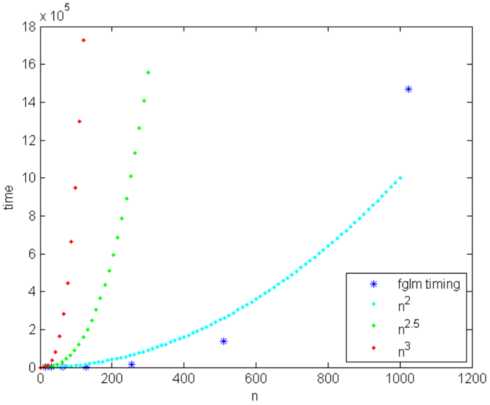

Figure : We use $G^{(lex)} = \left\{ \prod_{i=1}^{n}(x - \alpha_i) \, , \; y - h_v(x) \right\}$ as input for FGLM algorithm to compute a GB with respect to $(1, k-1)$-weighted degree ordering.

Future work

Compute the staircase of $I(\mathcal{A})$ wrt $(1, k-1)$-weighted degree ordering

$$
\begin{array}{ccc}
1 & & \\
x & & \\
x^2 & & \\
\vdots & & \\
x^{k-2} & & \\
x^{k-1} & y & \\
x^k & xy & \\
x^{k+1} & x^2y & \\
\vdots & \vdots & \\
x^{2k-3} & x^{k-2}y & \\
x^{2k-2} & x^{k-1}y & y^2 \\
x^{2k-1} & x^k y & xy^2 \\
x^{2k} & x^{k+1}y & x^2y^2 \\
\vdots & \vdots & \vdots \\
x^{3k-4} & x^{2k-3}y & x^{k-2}y^2
\end{array}
$$

Future work

Compute the staircase of $I(\mathcal{A})$ wrt $(1, k-1)$-weighted degree ordering

$$
\begin{array}{ccc}
1 & & \\
x & & \\
x^2 & & \\
\vdots & & \\
x^{k-2} & & \\
x^{k-1} & y & \\
x^k & xy & \\
x^{k+1} & x^2y & \\
\vdots & \vdots & \\
x^{2k-3} & x^{k-2}y & \\
x^{2k-2} & x^{k-1}y & y^2 \\
x^{2k-1} & x^ky & xy^2 \\
x^{2k} & x^{k+1}y & x^2y^2 \\
\vdots & \vdots & \vdots \\
x^{3k-4} & x^{2k-3}y & x^{k-2}y^2
\end{array}
$$

$$
\begin{array}{ccccccc}
\vdots & & & & & & \\
* & * & * & * & * & & \\
* & * & * & * & * & * & \\
* & * & * & \mathrm{m} & \star & \star & \\
\star & \star & \star & * & * & * & \\
* & * & * & * & * & * & \\
\vdots & & & & & & \\
* & * & * & * & * & * & \star
\end{array}
\qquad
\begin{array}{ccccccc}
\vdots & & & & & & \\
* & * & * & * & * & & \\
* & * & * & \mathrm{m} & \star & \star & \\
\star & \star & \star & * & * & * & \\
* & * & * & * & * & * & \\
* & * & * & * & * & * & \\
\vdots & & & & & & \\
* & * & * & * & * & * & *
\end{array}
$$


That's all Folks!