Faster Algorithms for List-Decoding Reed-Solomon Codes via Simultaneous Polynomial Approximations

Vincent NEIGER[§,†]

Claude-Pierre JEANNEROD[§] Éric SCHOST[†] Gilles VILLARD[§]

[§]AriC, LIP, École Normale Supérieure de Lyon, France

[†]ORCCA, Computer Science Department, Western University, London, ON, Canada

Aric Tuesday Work Session
July 1st, 2014

Outline

1. Unique decoding via approximation
   - Encoding and transmission
   - Unique decoding
   - Berlekamp-Welch(-like) algorithm
2. List-decoding Reed-Solomon codes
   - List-decoding
   - The interpolation step (previous work)
3. List-decoding via approximation
   - From interpolation to approximation
   - Solving the approximation problem using structured matrices
   - Extension to the multivariate case (folded Reed-Solomon codes)

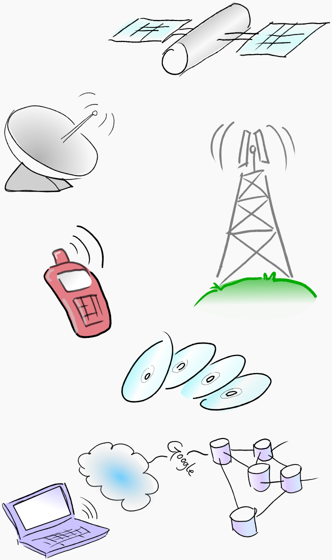
Outline

1. Unique decoding via approximation
   - Encoding and transmission
   - Unique decoding
   - Berlekamp-Welch(-like) algorithm
2. List-decoding Reed-Solomon codes
   - List-decoding
   - The interpolation step (previous work)
3. List-decoding via approximation
   - From interpolation to approximation
   - Solving the approximation problem using structured matrices
   - Extension to the multivariate case (folded Reed-Solomon codes)

Error-correcting codes

Goal:
Enable reliable delivery of data over unreliable communication channels

Strategy:
add redundancy to the message
add redundancy to the message
add redundancy to the message

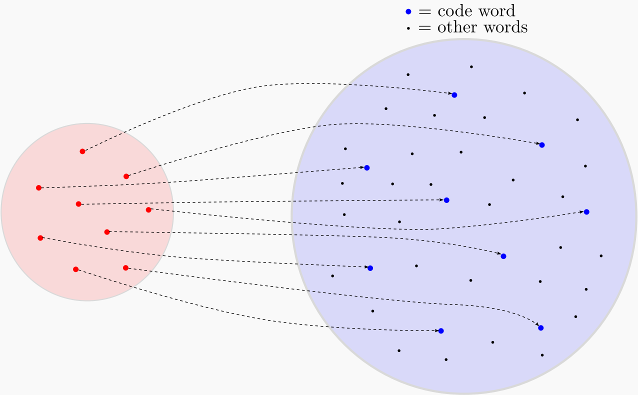


(courtesy of J.S.R. Nielsen)

Encoding: adding redundancy

All intended words $\longrightarrow$ All code words

$(w_0, \ldots, w_k)$ $\quad$ $(c_1, \ldots, c_n)$



polynomials of degree $\leqslant k$ $\longrightarrow$ their evaluation at $x_1, \ldots, x_n$

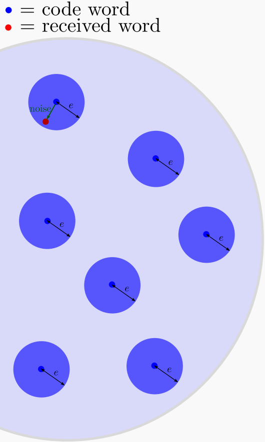
$w = w_0 + w_1 X + \cdots + w_k X^k$ $\quad$ $(w(x_1), \ldots, w(x_n))$

Transmission over an unreliable channel

Assumption: there are at most e errors during transmission of a code word

$$c = (c_1, \ldots, c_n) \xrightarrow{\text{noise}} y = (y_1, \ldots, y_n)$$

with $\#\{i \mid c_i \neq y_i\} \leqslant e$ (metric called Hamming distance)



Transmission over an unreliable channel

Assumption: there are at most e errors during transmission of a code word

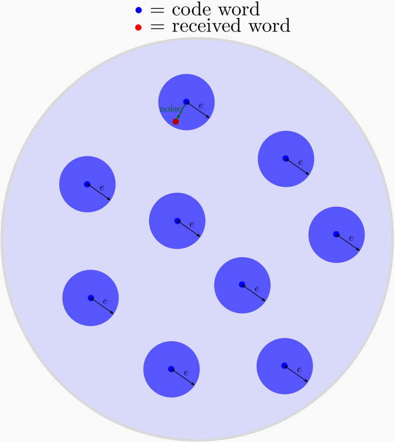
$$c = (c_1, \ldots, c_n) \xrightarrow{\text{noise}} y = (y_1, \ldots, y_n)$$

with $\#\{i \mid c_i \neq y_i\} \leqslant e$ (metric called Hamming distance)

Reed-Solomon code:
$(w(x_1), \ldots, w(x_n)) \xrightarrow{\text{noise}} (y_1, \ldots, y_n)$
with $\#\{i \mid w(x_i) \neq y_i\} \leqslant e$

$(y_1, \ldots, y_n)$ is the received word

All possible received words = words in the balls of radius e centered on the code words

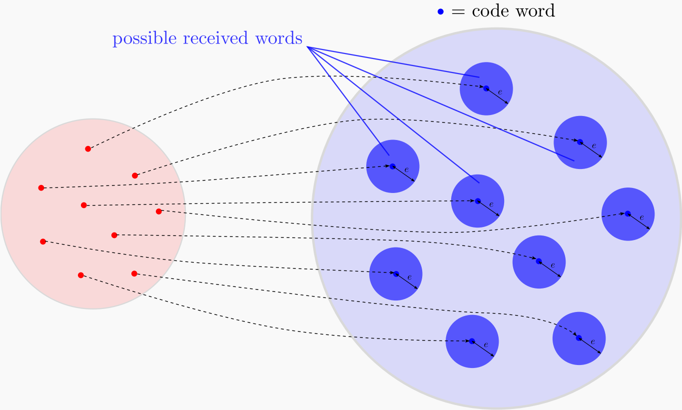


Transmission over an unreliable channel

Assumption: there are at most e errors during transmission of a code word

$$c = (w(x_1), \ldots, w(x_n)) \xrightarrow{\text{noise}} y = (y_1, \ldots, y_n)$$

with $\#\{i \mid w(x_i) \neq y_i\} \leqslant e$ (metric called Hamming distance)



Unique decoding

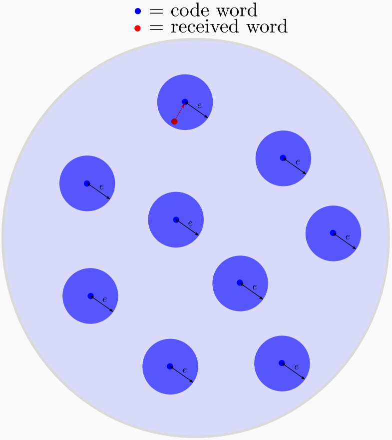
Received word $(y_1, \ldots, y_n)$

Decoding

find a polynomial w of degree $\leqslant k$ such that $\#\{i \mid w(x_i) \neq y_i\} \leqslant e$

Well-defined?

Exactly one such polynomial w as long as no overlap between the balls of radius e centered on the codewords



Unique decoding

Received word $(y_1, \ldots, y_n)$

Decoding

find a polynomial w of degree $\leqslant k$ such that $\#\{i \mid w(x_i) \neq y_i\} \leqslant e$

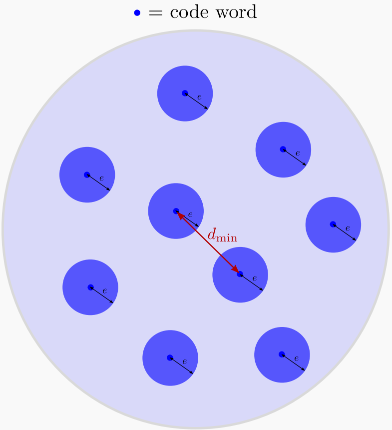
Well-defined?

Exactly one such polynomial w as long as no overlap between the balls of radius e centered on the codewords

Unique decoding

when

$$2e < d_{\min}$$



Unique decoding

Received word $(y_1, \ldots, y_n)$

Decoding

find a polynomial w of degree $\leqslant k$ such that $\#\{i \mid w(x_i) \neq y_i\} \leqslant e$

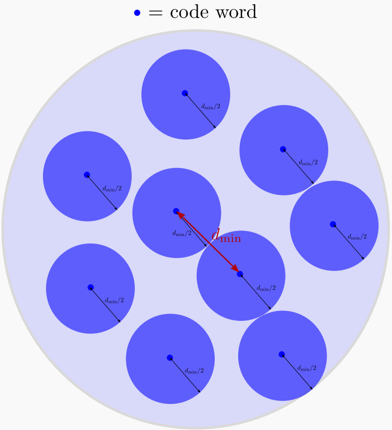
Well-defined?

Exactly one such polynomial w as long as no overlap between the balls of radius e centered on the codewords

Unique decoding

when

$$2e < d_{\min}$$



Minimum distance

For Reed-Solomon codes:

- for $w_1 \neq w_2$ polynomials of degree $\leqslant k$ over the base field $\mathbb{K}$, $(w_1(x_1), \ldots, w_1(x_n))$ and $(w_2(x_1), \ldots, w_2(x_n))$ agree at $\leqslant k$ positions
$\Rightarrow$ distance at least $n - k$ between two code words
- for $w_1 = 0$ and $w_2 = (X - x_1) \cdots (X - x_k)$, the code words are $(0, \ldots, 0)$ and $(0, \ldots, 0, w_2(x_{k+1}), \ldots, w_2(x_n))$
$\Rightarrow$ two code words at distance exactly $n - k$

$\Longrightarrow$ minimum distance $d_{\min} = n - k$

Hence the unique decoding condition: $e < \dfrac{n-k}{2}$

Unique decoding problem

Unique decoding of Reed-Solomon codes

Input:

$x_1, \ldots, x_n$ the n distinct evaluation points in $\mathbb{K}$,
k the degree bound, e the error-correction radius,
$(y_1, \ldots, y_n)$ the received word in $\mathbb{K}^n$

Unique decoding assumption: $e < \frac{n-k}{2}$

Output:

The polynomial w in $\mathbb{K}[X]$ such that

$$\deg w \leqslant k \qquad \text{and} \qquad \#\{i \mid w(x_i) \neq y_i\} \leqslant e.$$

Key equations (unique decoding)

Define the interpolation polynomial

$$R(X) \text{ such that } R(x_i) = y_i,$$

and the error-locator polynomial

$$\Lambda(X) = \prod_{i \mid \text{error}} (X - x_i).$$

$\Lambda(X)$ is an unknown polynomial with $\deg \Lambda \leqslant e$

Key equations

$$\text{for every } i, \quad \Lambda(x_i)R(x_i) \;=\; \Lambda(x_i)w(x_i)$$

Quadratic equations in the unknown coefficients of w and Λ...

Modular key equation (unique decoding)

Interpolation polynomial and error-locator polynomial

$$R(x_i) = y_i, \qquad \Lambda(X) = \prod_{i \mid \text{error}} (X - x_i)$$

Key equations

$$\text{for every } i, \quad \Lambda(x_i)R(x_i) = \Lambda(x_i)w(x_i)$$

i.e. for every i, $\Lambda(X)R(X) = \Lambda(X)w(X) \mod (X - x_i)$

Modular key equation (unique decoding)

Interpolation polynomial and error-locator polynomial

$$R(x_i) = y_i, \qquad \Lambda(X) = \prod_{i \mid \text{error}} (X - x_i)$$

Key equations

$$\text{for every } i, \quad \Lambda(x_i) R(x_i) = \Lambda(x_i) w(x_i)$$

i.e. for every i, $\Lambda(X) R(X) = \Lambda(X) w(X) \mod (X - x_i)$
Define the master polynomial

$$G(X) = \prod_{1 \leqslant i \leqslant n} (X - x_i)$$

Modular key equation

$$\Lambda(X) R(X) = \Lambda(X) w(X) \mod G(X)$$

Unique decoding via rational reconstruction

Modular key equation:

$$\Lambda R = \Lambda w \mod G$$

where $R(x_i) = y_i$, $G(X) = \prod_{1 \leqslant i \leqslant n}(X - x_i)$, $\Lambda(X) = \prod_{i \mid \text{error}}(X - x_i)$.

$\Longrightarrow \lambda = \Lambda, \omega = \Lambda w$ form a solution of the rational reconstruction problem

$$\begin{cases} \lambda R = \omega \mod G, \\ \deg(\lambda) \leqslant e, \quad \deg(\omega) < n - e, \quad \lambda \text{ monic.} \end{cases}$$

(since $\deg \Lambda w \leqslant e + k < n - e$ by the unique decoding assumption)

[Modern Computer Algebra, von zur Gathen - Gerhard, 2003]

Berlekamp-Welch(-like) algorithm for unique decoding

$\lambda = \Lambda, \omega = \Lambda w$ form a solution of the rational reconstruction problem

$$\begin{cases} \lambda R = \omega \mod G, \\ \deg(\lambda) \leqslant e, \quad \deg(\omega) < n - e, \quad \lambda \text{ monic.} \end{cases}$$

$\Longrightarrow$ unique rational solution ω/λ, which has to be $\frac{\Lambda w}{\Lambda} = w$!

This solution is computed using the extended Euclidean algorithm in $\mathcal{O}\tilde{}(n)$ operations in $\mathbb{K}$

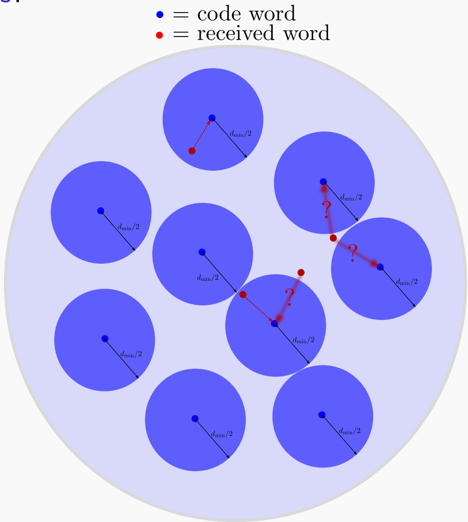
Conclusion:
unique decoding in quasi-linear time via an approximation problem

Outline

Non-unique decoding

How to "decode" when more errors?

transmission with $\leqslant e$ errors
where $e \geqslant d_{\min}/2$



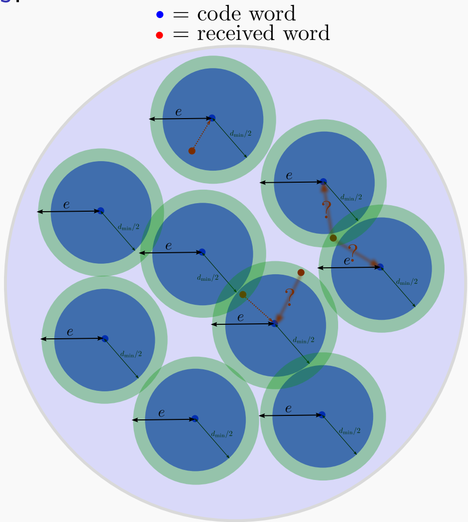
Non-unique decoding

How to "decode" when more errors?

transmission with $\leqslant e$ errors
where $e \geqslant d_{\min}/2$

possibly two (or more) code words at the same distance...

the closest code word is not necessarily the one which was sent...



Non-unique decoding

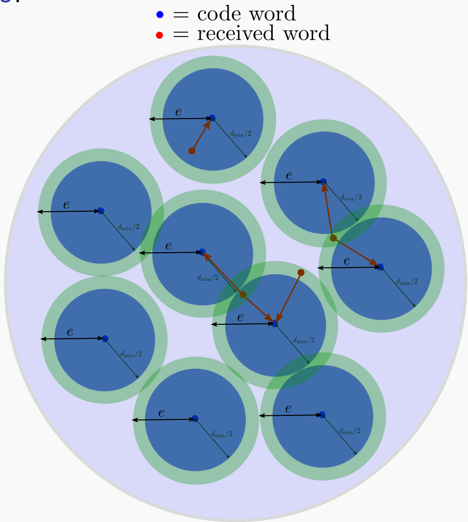
How to "decode" when more errors?

transmission with $\leqslant e$ errors
where $e \geqslant d_{\min}/2$

possibly two (or more) code words
at the same distance...

the closest code word is not necessarily the one which was sent...

$\Rightarrow$ Return a list of all code words
at distance $\leqslant e$
(called list-decoding)



List-decoding problem

For convenience, we use the agreement parameter $t = n - e$

List-decoding Reed-Solomon codes

Input:

n points $\{(x_i, y_i)\}_{1 \leqslant i \leqslant n}$ in $\mathbb{K}^2$, with the x_i's distinct

k the degree constraint, t the agreement

List-decoding assumption: $t^2 > kn$ [Guruswami - Sudan 1999]

Output:

all polynomials w in $\mathbb{K}[X]$ such that

$$\deg w \leqslant k \qquad \text{and} \qquad \#\{i \mid w(x_i) = y_i\} \geqslant t.$$

Problem also called *Polynomial Reconstruction*

Polynomial Reconstruction

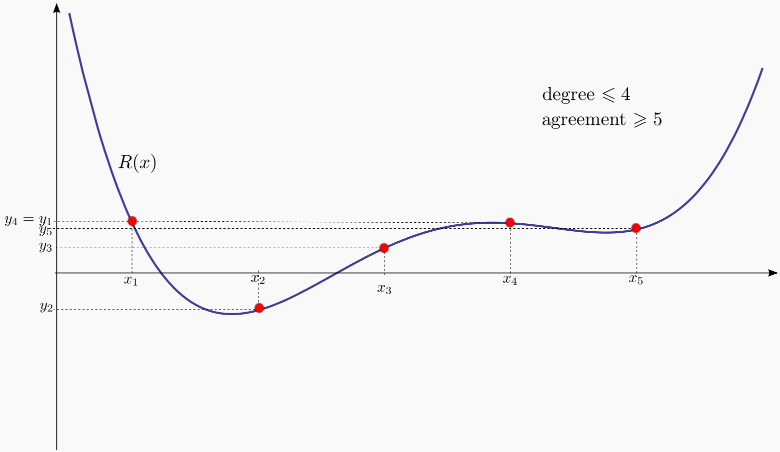


Figure: Polynomial reconstruction (Lagrange interpolation)

Polynomial Reconstruction

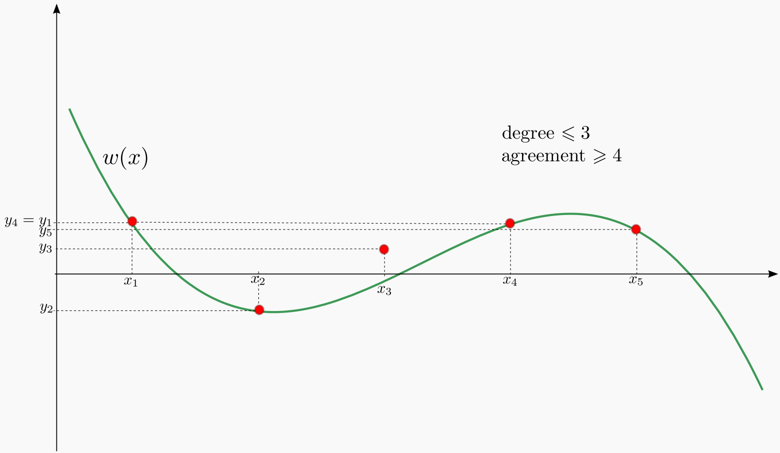


Figure: Polynomial reconstruction

Polynomial Reconstruction

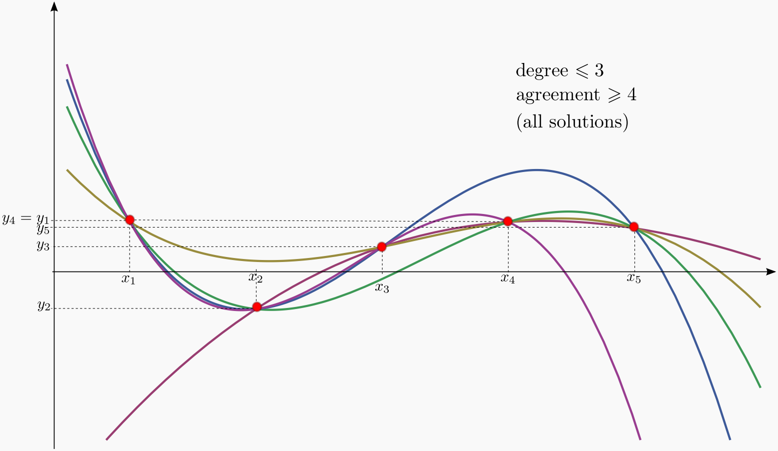


Figure: Polynomial reconstruction (all solutions)

Why the interpolation step (1/3)

Consider one solution w_1. We still have the modular key equation

$$\Lambda_1 R \;=\; \Lambda_1 w_1 \quad \text{mod } G$$

where
$R(x_i) = y_i, \quad G(X) = \prod_{1 \leqslant i \leqslant n}(X - x_i), \quad \Lambda_1(X) = \prod_{i \mid \text{error}_1}(X - x_i).$

But possibly,

$$\deg(\Lambda_1) + \deg(\Lambda_1 w_1) \;\geqslant\; n = \deg G$$

$\Longrightarrow$ no uniqueness of a rational solution ω_1/λ_1 to the problem

$$\lambda_1 R \;=\; \omega_1 \quad \text{mod } G \text{ with } \deg \omega_1 \leqslant e + k$$

(more unknowns than equations in the linearized problem)

Why the interpolation step (2/3)

Note that

$$\Lambda_1(R - w_1) \;=\; 0 \quad \bmod G$$

Now consider two solutions w_1, w_2. We have the modular key equation

$$\Lambda(R - w_1)(R - w_2) \;=\; 0 \quad \bmod G$$

where $\Lambda = \prod_{i \mid \text{error}_{1\wedge 2}}(X - x_i) = \gcd(\Lambda_1, \Lambda_2)$.

$\Longrightarrow$ w_1, w_2 are Y-roots of the bivariate polynomial

$$Q(X, Y) \;=\; \Lambda(Y - w_1)(Y - w_2)$$

Why the interpolation step (3/3)

Consider two solutions w_1, w_2, then $\Lambda(R - w_1)(R - w_2) = 0 \mod G$ and w_1, w_2 are Y-roots of

$$\begin{aligned} Q(X,Y) &= \Lambda(Y - w_1)(Y - w_2) \\ &= \Lambda w_1 w_2 - \Lambda(w_1 + w_2)Y + \Lambda Y^2 \end{aligned}$$

Similar remark when considering all ℓ solutions $w_1, \ldots, w_\ell$

Properties of $Q(X,Y)$:

- the unknown degree in Y of $Q(X,Y)$ is the number of solutions ℓ
- the unknown coefficients in X of $Q(X,Y)$ have small degree
- we have the modular identity $Q(X,R) = 0 \mod G$ or equivalently, for every i, $Q(x_i, y_i) = 0$

Guruswami-Sudan algorithm

It consists of two main steps,

- Interpolation step
  compute $Q(X, Y)$ such that: $w(X)$ solution $\Rightarrow Q(X, w(X)) = 0$
- Root-finding step
  find all Y**-roots of** $Q(X, Y)$, keep those that are solutions

Here we are interested in the interpolation step
$\Rightarrow$ leads to a problem of **Interpolation with Multiplicities**.

A problem of Interpolation with multiplicities

Interpolation With Multiplicities

Input:

n points $\{(x_i, y_i)\}_{1 \leqslant i \leqslant n}$ in $\mathbb{K}^2$, with the x_i's distinct

k the degree constraint, t the agreement

ℓ the list-size, m the multiplicity $(m \leqslant \ell)$

Output:

a polynomial Q in $\mathbb{K}[X, Y]$ such that

(i)	Q is nonzero,	
(ii)	$\deg_Y Q(X, Y) \leqslant \ell$,	(list-size condition)
(iii)	$\deg_X Q(X, X^k Y) < mt$,	(weighted-degree condition)
(iv)	$\forall i,\ Q(x_i, y_i) = 0$ with multiplicity m.	(vanishing condition)

Algorithms based on structured linear systems

[Roth - Ruckenstein, 2000] [Zeh - Gentner - Augot, 2011]

Write

$$Q(X,Y) = \sum_{0\leqslant j\leqslant \ell} Q_j(X) Y^j \qquad \text{(list-size condition)}$$

$$\text{where} \quad \deg Q_j(X) < mt - jk. \qquad \text{(weighted-degree condition)}$$

Then, rewrite the vanishing condition so that a solution $Q(X,Y)$ can be retrieved as a nontrivial solution of a homogeneous mosaic-Hankel linear system (the unknown being the coefficient vector of $Q(X,Y)$).

Complexity bound for this method:

$$\mathcal{O}(\ell m^4 n^2)$$

using a modified Feng-Tzeng's linear system solver [Feng - Tzeng, 1991].

Algorithms based on polynomial lattices

[Alekhnovich, 2002] [Reinhard, 2003] [Beelen - Brander, 2010]
[Bernstein, 2011] [Cohn - Heninger, 2011]

Build a polynomial lattice $\mathcal{L}$ such that

$$Q(X, Y) \in \mathcal{L} \quad \Leftrightarrow \quad \text{(list-size condition)} + \text{(vanishing condition)}.$$

Then, a solution to Interpolation With Multiplicities can be retrieved as a short vector in $\mathcal{L}$ (weighted-degree condition).

Complexity bound for this method:

$$\mathcal{O}\tilde{}(\ell^\omega mn)$$

using an efficient polynomial lattice basis reduction algorithm:
[Giorgi - Jeannerod - Villard, 2003] (probabilistic)
or [Gupta - Sarkar - Storjohann - Valeriote, 2012]

Contributions

[Chowdhury - Jeannerod - Neiger - Schost - Villard, 2014]

1. New approach for the interpolation step
   - Based on a approximation problem
   - Solved using structured linear systems
   - Improved complexity bound

$$\mathcal{O}\tilde{~}(\ell^{\omega-1} m^2 n)$$

2. Extension to the multivariate case (folded Reed-Solomon codes)
   - Based on the same approximation problem
   - Improved complexity bound

$$\mathcal{O}\tilde{~}\left(\binom{s+\ell}{s}^{\omega-1} mn \binom{s+m-1}{s}\right)$$

Outline

Contributions

[Chowdhury - Jeannerod - Neiger - Schost - Villard, 2014]

1. New approach for the interpolation step
   - Based on a approximation problem
   - Solved using structured linear systems
   - Improved complexity bound

$$\mathcal{O}\tilde{}(\ell^{\omega-1} m^2 n)$$

2. Extension to the multivariate case (folded Reed-Solomon codes)
   - Based on the same approximation problem
   - Improved complexity bound

$$\mathcal{O}\tilde{}\left(\binom{s+\ell}{s}^{\omega-1} mn \binom{s+m-1}{s}\right)$$

Reduction to an approximation problem (1/2)

Assume that Q satisfies the list-size condition:

$$Q = \sum_{j \leqslant \ell} Q_j(X) Y^j$$

for some unknown polynomials $Q_0, \ldots, Q_\ell$

The vanishing condition can be rewritten as a set of modular equations

$$\forall i \in \{1, \ldots, n\},\; Q(x_i, y_i) = 0 \text{ with multiplicity } m$$

$$\iff \quad \forall i < m, \quad \sum_{i \leqslant j \leqslant \ell} Q_j(X) \binom{j}{i} R(X)^{j-i} \; = \; 0 \mod G(X)^{m-i}$$

where $G(X) = \prod_{1 \leqslant i \leqslant n}(X - x_i)$ and $R(X)$ such that $\forall i, R(x_i) = y_i$.

Reduction to an approximation problem (2/2)

Vanishing condition + list-size condition

$$\forall i < m, \qquad \sum_{i \leqslant j \leqslant \ell} Q_j(X) \underbrace{\binom{j}{i} R(X)^{j-i}}_{F_{i,j}(X)} = 0 \pmod{\underbrace{G(X)^{m-i}}_{P_i(X)}}$$

Cost for computing $F_{i,j}$ and P_i:

- computing $n(m-i)$ coefficients of $F_{i,j}$ for every i, j
  $\approx$ computing nm coefficients of $R(X)^j$ for $0 \leqslant j \leqslant \ell$
  $\rightsquigarrow$ $\tilde{\mathcal{O}}(\ell m^2 n)$ **operations** $\quad \in \mathcal{O}(\ell^{\omega-1} m^2 n)$
- computing P_i for every i
  $=$ computing the m polynomials $G(X), G(X)^2, \ldots, G(X)^m$
  $\rightsquigarrow$ $\tilde{\mathcal{O}}(m^2 n)$ **operations** $\quad \in \mathcal{O}(\ell^{\omega-1} m^2 n)$

Reduction to an approximation problem (2/2)

Vanishing condition + list-size condition + weighted-degree condition

$$\forall i < m, \qquad \sum_{i \leqslant j \leqslant \ell} Q_j(X) \underbrace{\binom{j}{i} R(X)^{j-i}}_{F_{i,j}(X)} = 0 \pmod{\underbrace{G(X)^{m-i}}_{P_i(X)}}$$

with the degree constraints $\deg Q_j(X) < mt - jk$ for $j \leqslant \ell$

Cost for computing $F_{i,j}$ and P_i:

- computing $n(m-i)$ coefficients of $F_{i,j}$ for every i, j
  $\approx$ computing nm coefficients of $R(X)^j$ for $0 \leqslant j \leqslant \ell$
  $\rightsquigarrow$ $\mathcal{O}\tilde{~}(\boldsymbol{\ell} \mathbf{m^2 n})$ **operations** $\quad \in \mathcal{O}(\ell^{\omega-1} m^2 n)$
- computing P_i for every i
  $=$ computing the m polynomials $G(X), G(X)^2, \ldots, G(X)^m$
  $\rightsquigarrow$ $\mathcal{O}\tilde{~}(\mathbf{m^2 n})$ **operations** $\quad \in \mathcal{O}(\ell^{\omega-1} m^2 n)$

The approximation problem

$$\forall i < m, \qquad \sum_{i \leqslant j \leqslant \ell} Q_j(X) \underbrace{\binom{j}{i} R(X)^{j-i}}_{F_{i,j}(X)} = 0 \pmod{\underbrace{G(X)^{m-i}}_{P_i(X)}}$$

with the degree constraints $\deg Q_j(X) < mt - jk$ for $j \leqslant \ell$

Simultaneous Polynomial Approximations

Input:

- Parameters: ℓ the list-size, m the number of equations
- Moduli: $P_i \in \mathbb{K}[X]$ monic of degree M_i, for every $i < m$
- Polynomials: $F_{i,j} \in \mathbb{K}[X]$ of degree less than M_i, for $i < m$ and $j \leqslant \ell$
- Degree bounds: N_j a positive integer, for every $j \leqslant \ell$

Output: $Q_0, \ldots, Q_\ell \in \mathbb{K}[X]$ satisfying

- (i') Q_j are not all zero,
- (ii') $\forall j \leqslant \ell$, $\deg Q_j < N_j$,
- (iii') $\forall i < m$, $\sum_{j \leqslant \ell} Q_j F_{i,j} = 0 \pmod{P_i}$.

Simultaneous approximations via a structured system (1/3)

Write $Q_j(X) = \sum_{r<N_j} Q_j^{(r)} X^r$, then the equations are

$$\forall i < m, \qquad \sum_{i \leqslant j \leqslant \ell} \sum_{r<N_j} Q_j^{(r)} X^r F_{i,j}(X) \ = \ 0 \pmod{P_i(X)}$$

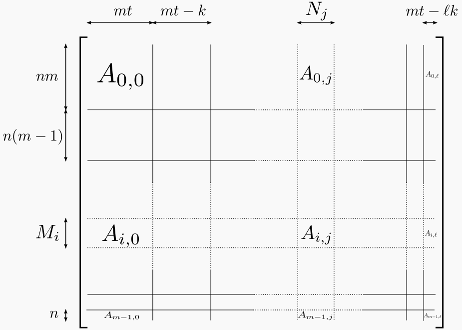
Define the companion matrix

$$\mathcal{C}(P_i) \ = \ \begin{bmatrix} 0 & 0 & \cdots & 0 & -P_i^{(0)} \\ 1 & 0 & \cdots & 0 & -P_i^{(1)} \\ 0 & 1 & \cdots & 0 & -P_i^{(2)} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -P_i^{(M_i-1)} \end{bmatrix} \ \in \ \mathbb{K}^{M_i \times M_i}$$

Key property:
multiplication by $\mathcal{C}(P_i)$ on the left is multiplication by X modulo $P_i(X)$

Simultaneous approximations via a structured system (2/3)

Solution $\iff$ nonzero vector in the nullspace of the matrix A



where the block $A_{i,j} \in \mathbb{K}^{M_i \times N_j}$ is defined by its first column

$$c^{(0)} = \begin{bmatrix} F_{i,j}^{(0)} \\ \vdots \\ F_{i,j}^{(M_i-1)} \end{bmatrix}$$ and the subsequent columns $c^{(r+1)} = \mathcal{C}(P_i) \cdot c^{(r)}$

Simultaneous approximations via a structured system (3/3)

Let $M = M_0 + \cdots + M_{m-1}$ (number of linear equations),
and $N = N_0 + \cdots + N_\ell$ (number of linear unknowns)
Define

$$\mathcal{Z}_M = \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{bmatrix} \in \mathbb{K}^{M \times M}$$

Fact: $A - \mathcal{Z}_M A \mathcal{Z}_N^T$ has rank $\leqslant m + \ell + 1$

the displacement operator $A \mapsto A - \mathcal{Z}_M A \mathcal{Z}_N^T$ corresponds to a Toeplitz structure

Conclusion:
the matrix of the system is Toeplitz-like with displacement rank $\leqslant 2\ell$

Complexity bound for this approach

Solving the structured linear system [Bitmead - Anderson, 1980] [Morf, 1980] [Kaltofen, 1994] [Pan, 2001] [Bostan - Jeannerod - Schost, 2007]

Two main operations:

- computing generators
  $\approx$ computing the first and last column of each block $\rightsquigarrow \tilde{\mathcal{O}}(\ell m^2 n)$
  $+$ computing the first row of each block $\rightsquigarrow \tilde{\mathcal{O}}(\ell m^2 n)$
  $\rightsquigarrow$ $\tilde{\mathcal{O}}(\boldsymbol{\ell m^2 n})$ **operations**
- solving the system
  at most $\ell + 1$ blocks on each row or column,
  the number of equations is $\sum_i n(m-i) = \mathcal{O}(m^2 n)$
  $\rightsquigarrow$ $\tilde{\mathcal{O}}(\boldsymbol{\ell^{\omega-1} m^2 n})$ **operations**

Complexity bound:

$$\tilde{\mathcal{O}}(\ell^{\omega-1} m^2 n)$$

Contributions

[Chowdhury - Jeannerod - Neiger - Schost - Villard, 2014]

1. New approach for the interpolation step
   - Based on a approximation problem
   - Solved using structured linear systems
   - Improved complexity bound

$$\mathcal{O}\tilde{}(\ell^{\omega-1} m^2 n)$$

2. Extension to the multivariate case (folded Reed-Solomon codes)
   - Based on the same approximation problem
   - Improved complexity bound

$$\mathcal{O}\tilde{}\left(\binom{s+\ell}{s}^{\omega-1} mn \binom{s+m-1}{s}\right)$$

Contributions

[Chowdhury - Jeannerod - Neiger - Schost - Villard, 2014]

1. New approach for the interpolation step
   - Based on a approximation problem
   - Solved using structured linear systems
   - Improved complexity bound

$$\mathcal{O}^{\sim}(\ell^{\omega-1} m^2 n)$$

2. Extension to the multivariate case (folded Reed-Solomon codes)
   - Based on the same approximation problem
   - Improved complexity bound

$$\mathcal{O}^{\sim}\left(\binom{s+\ell}{s}^{\omega-1} mn \binom{s+m-1}{s}\right)$$

Multivariate Interpolation with Multiplicities

Multivariate Interpolation With Multiplicities

Input:

- s the number of variables
- n points $\{(x_i, y_{i1}, \ldots, y_{is})\}_{1 \leqslant i \leqslant n}$ in $\mathbb{K}^{s+1}$, with the x_i's distinct
- k the degree constraint, t the agreement
- ℓ the list-size, m the multiplicity

Output: a polynomial Q in $\mathbb{K}[X, Y_1, \ldots, Y_s]$ such that

(i) Q is nonzero,

(ii) $\deg_{\boldsymbol{Y}} Q(X, Y_1, \ldots, Y_s) \leqslant \ell$, (list-size condition)

(iii) $\deg_X Q(X, X^k Y_1, \ldots, X^k Y_s) < mt$, (weighted-degree condition)

(iv) $\forall i,\ Q(x_i, y_{i1}, \ldots, y_{is}) = 0$ with multiplicity m. (vanishing condition)

Application: list-decoding of folded Reed-Solomon codes

Reduction to an approximation problem (1/2)

Assume that Q satisfies the list-size condition:

$$Q = \sum_{|\boldsymbol{j}| \leqslant \ell} Q_{\boldsymbol{j}}(X) Y^{\boldsymbol{j}}$$

for some unknown polynomials $\{Q_{\boldsymbol{j}}, \ |\boldsymbol{j}| \leqslant \ell\}$

The vanishing condition can be rewritten as a set of modular equations.

$$\text{for } i \in \{1, \ldots, n\} : \ Q(x_i, y_{i1}, \ldots, y_{is}) = 0 \text{ with multiplicity } m$$

$$\iff \quad \text{for } \boldsymbol{i} = (i_1, \ldots, i_s), \ |\boldsymbol{i}| < m :$$

$$\sum_{\boldsymbol{i} \preccurlyeq \boldsymbol{j}, |\boldsymbol{j}| \leqslant \ell} Q_{\boldsymbol{j}}(X) \binom{j_1}{i_1} R_1(X)^{j_1 - i_1} \cdots \binom{j_s}{i_s} R_s(X)^{j_s - i_s} = 0 \mod G(X)^{m - |\boldsymbol{i}|}$$

where $G(X) = \prod_{1 \leqslant i \leqslant n} (X - x_i)$ and

$$R_1(X), \ldots, R_s(X) \text{ such that } R_1(x_i) = y_{i1}, \ldots, R_s(x_i) = y_{is}$$

Reduction to an approximation problem (2/2)

Vanishing condition + list-size condition

$$\sum_{\boldsymbol{i} \preccurlyeq \boldsymbol{j}, |\boldsymbol{j}| \leqslant \ell} Q_{\boldsymbol{j}}(X) \underbrace{\binom{j_1}{i_1} R_1(X)^{j_1 - i_1} \cdots \binom{j_s}{i_s} R_s(X)^{j_s - i_s}}_{F_{\boldsymbol{i},\boldsymbol{j}}(X)} = 0 \mod \underbrace{G(X)^{m-|\boldsymbol{i}|}}_{P_{\boldsymbol{i}}(X)}$$

for $\boldsymbol{i} = (i_1, \ldots, i_m)$ such that $|\boldsymbol{i}| < m$,

Instance of Simultaneous Polynomial Approximations

- list-size $\binom{s+\ell}{s}$
- number of linear equations $mn\binom{s+m-1}{s}$

Reduction to an approximation problem (2/2)

Vanishing condition + list-size condition + weighted-degree condition

$$\sum_{\boldsymbol{i} \preccurlyeq \boldsymbol{j}, |\boldsymbol{j}| \leqslant \ell} Q_{\boldsymbol{j}}(X) \underbrace{\binom{j_1}{i_1} R_1(X)^{j_1 - i_1} \cdots \binom{j_s}{i_s} R_s(X)^{j_s - i_s}}_{F_{\boldsymbol{i},\boldsymbol{j}}(X)} = 0 \mod \underbrace{G(X)^{m-|\boldsymbol{i}|}}_{P_{\boldsymbol{i}}(X)}$$

for $\boldsymbol{i} = (i_1, \ldots, i_m)$ such that $|\boldsymbol{i}| < m$,
with the degree constraints $\deg Q_{\boldsymbol{j}}(X) < mt - |\boldsymbol{j}|k$ for $|\boldsymbol{j}| \leqslant \ell$

Instance of Simultaneous Polynomial Approximations

- list-size $\binom{s+\ell}{s}$
- number of linear equations $mn\binom{s+m-1}{s}$

Complexity bound in the multivariate case

⇝ Complexity bound in the multivariate case

$$\tilde{\mathcal{O}}\left(\binom{s+\ell}{s}^{\omega-1} mn \binom{s+m-1}{s}\right)$$

Improves on [Busse, 2008], [Brander, 2010] and [Nielsen, 2014]

Further extends to

- weight specific to each variable
  $\deg_X Q(X, X^{k_1} Y_1, \ldots, X^{k_s} Y_s) < mt$
- multiplicity specific to each point
  $Q(x_i, y_{i1}, \ldots, y_{is}) = 0$ with multiplicity m_i

Contributions

[Chowdhury - Jeannerod - Neiger - Schost - Villard, 2014]

1. New approach for the interpolation step
   - Based on a approximation problem
   - Solved using structured linear systems
   - Improved complexity bound

$$\mathcal{O}\tilde{}(\ell^{\omega-1} m^2 n)$$

2. Extension to the multivariate case (folded Reed-Solomon codes)
   - Based on the same approximation problem
   - Improved complexity bound

$$\mathcal{O}\tilde{}\left(\binom{s+\ell}{s}^{\omega-1} mn \binom{s+m-1}{s}\right)$$

Contributions

[Chowdhury - Jeannerod - Neiger - Schost - Villard, 2014]

1. New approach for the interpolation step
    - Based on a approximation problem
    - Solved using structured linear systems
    - Improved complexity bound

$$\mathcal{O}\tilde{~}(\ell^{\omega-1} m^2 n)$$

2. Extension to the multivariate case (folded Reed-Solomon codes)
    - Based on the same approximation problem
    - Improved complexity bound

$$\mathcal{O}\tilde{~}\left(\binom{s+\ell}{s}^{\omega-1} mn \binom{s+m-1}{s}\right)$$