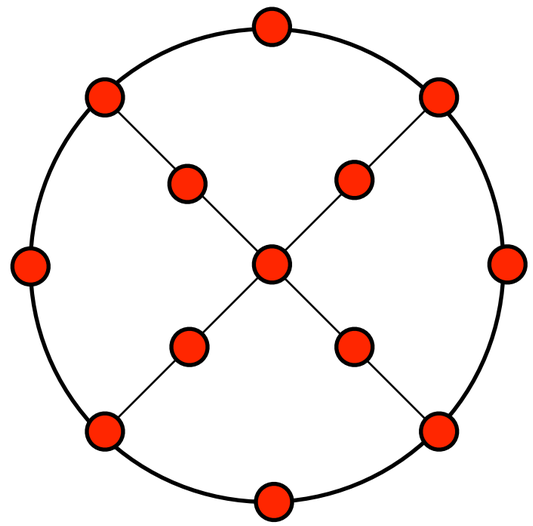
algo lma
laboratoire d'algorithmique
laboratoire de mathématiques algorithmique

Algebraic Decoding Algorithms



Amin Shokrollahi

EPFL
ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Reed-Solomon Codes

$\alpha_1, \ldots, \alpha_n$ distinct elements of $\mathbb{F}_q$

$$\begin{array}{ccc} \mathbb{F}_q[x]_{<k} & \longrightarrow & \mathbb{F}_q^n \\ (f_0, \ldots, f_{k-1}) & \longmapsto & (f(\alpha_1), \ldots, f(\alpha_n)) \end{array}$$

Image is a code of length n, dimension k, and minimum distance n-k+1. (If k is at most n.)

Proof: Polynomial of degree $<k$ has at most k-1 roots.

Encoding/Decoding

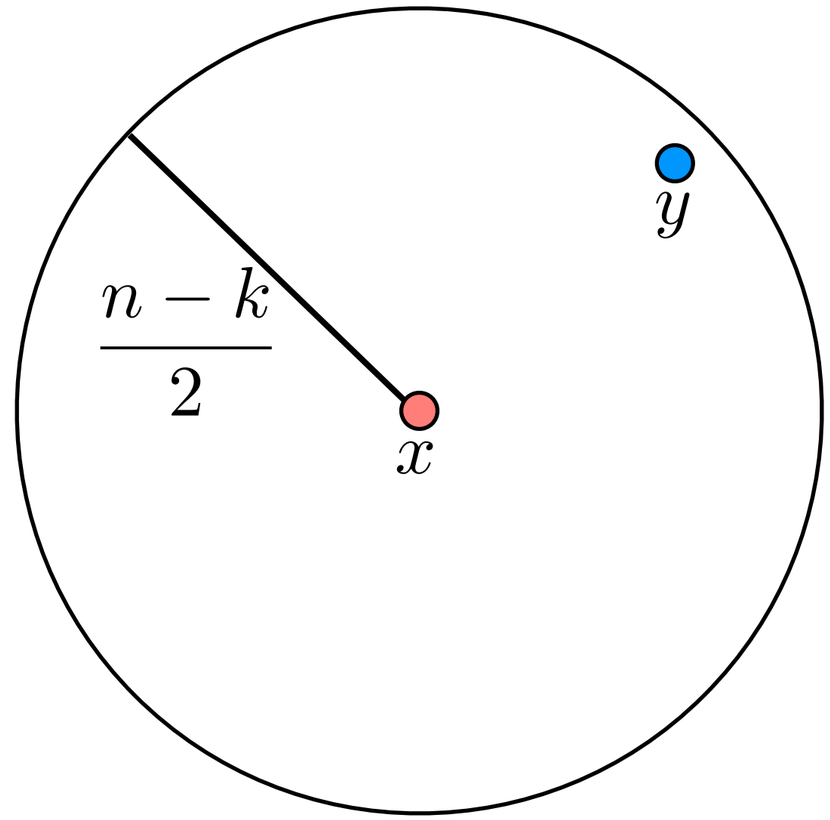
Encoding is trivial (multiple evaluation of a polynomial).

Decoding problem:

$x = (f(\alpha_1), \ldots, f(\alpha_n))$ sent.

$y = (y_1, \ldots, y_n)$ received.

Promise: $\#\{i \mid f(\alpha_i) \neq y_i\} \leq \dfrac{n-k}{2}$



Problem: Reconstruct f from y.

Welch-Berlekamp Decoder

$E = \{i \mid f(\alpha_i) \neq y_i\}$ Error set

$h \in \mathbb{F}_q[x]_{\leq \frac{n-k}{2}}$ Error locator polynomial:

$$h(x) = \prod_{i \in E} (x - \alpha_i)$$

$$\forall\, i: \quad h(\alpha_i)(f(\alpha_i) - y_i) = 0.$$

0 if i not in error

0 if i in error

Welch-Berlekamp Decoder

Find $(0,0) \neq (g,h) \in \mathbb{F}_q[x]_{<\frac{n+k}{2}} \times \mathbb{F}_q[x]_{\leq\frac{n-k}{2}}$ such that

$$\forall\, i : g(\alpha_i) - h(\alpha_i) y_i = 0$$

Then: $f = \frac{g}{h}$!

$g(x) - f(x)h(x)$ has degree less than $\frac{n+k}{2}$ but has at least $\frac{n+k}{2}$ roots, so is zero.

Existence and Computation

$$m = \frac{n+k}{2}, \qquad e = \frac{n-k}{2}$$

$$\left[\begin{array}{cccc|cccc} 1 & \alpha_1 & \cdots & \alpha_1^{m-1} & -1 & -y_1\alpha_1 & \cdots & -y_1\alpha_1^e \\ 1 & \alpha_2 & \cdots & \alpha_2^{m-1} & -1 & -y_2\alpha_2 & \cdots & -y_2\alpha_2^e \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \cdots & \alpha_n^{m-1} & -1 & -y_n\alpha_n & \cdots & -y_n\alpha_n^e \end{array}\right] \left[\begin{array}{c} g_0 \\ g_1 \\ \vdots \\ g_{m-1} \\ \hline h_0 \\ h_1 \\ \vdots \\ h_e \end{array}\right] = 0$$

n rows, *n*+1 columns, nonzero solution exists!

AG-Codes

RS	AG
Affine line	Smooth algebraic curve $\mathcal{X}$
$\alpha_1, \ldots, \alpha_n$	$P_1, \ldots, P_n \in \mathcal{X}(\mathbb{F}_q)$
Polynomials of degree $< k$	$\mathcal{L}(dQ), Q \in \mathcal{X}(\mathbb{F}_q)$

$$\begin{array}{rcl} \mathcal{L}(dQ) & \longrightarrow & \mathbb{F}_q^n \\ f & \longmapsto & (f(P_1), \ldots, f(P_n)) \end{array}$$

Parameters

Nonzero function in $\mathcal{L}(dQ)$ can have at most d zeros

$+$

Theorem of Riemann

$\dim \mathcal{L}(dQ) \geq d - g + 1$

$\Downarrow$

Dimension $\geq d - g + 1$

Minimum distance $\geq n - d$

WB-Decoder (S-Wasserman)

$$e = \frac{n-d+g-1}{2}$$

Find $(0,0) \neq (u,v) \in \mathcal{L}((e+d)Q) \times \mathcal{L}(eQ)$ such that

$$\forall\, i: \quad u(P_i) - y_i v(P_i) = 0$$

If number of errors $\leq \frac{n-d-g-1}{2}$, then correct codeword is given by

$$f = \frac{u}{v}$$

WB-Decoder (S-Wasserman)

Proof:

u, v exist: $\deg(eQ - \sum_{i \in E} P_i) \geq g$

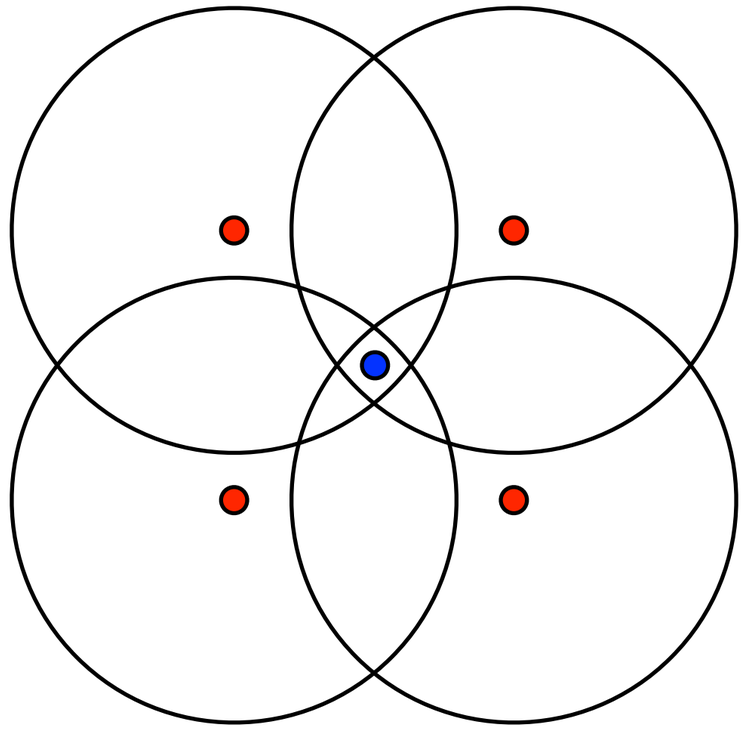
$u - fv = 0$: $\deg((e+d)Q - \sum_{i \notin E} P_i) < 0$

Facit

Most algorithms for decoding RS-codes can be generalized appropriately to the case of AG-codes.

Will concentrate on RS-codes in the following.

Decoding More Errors?



List-decoding

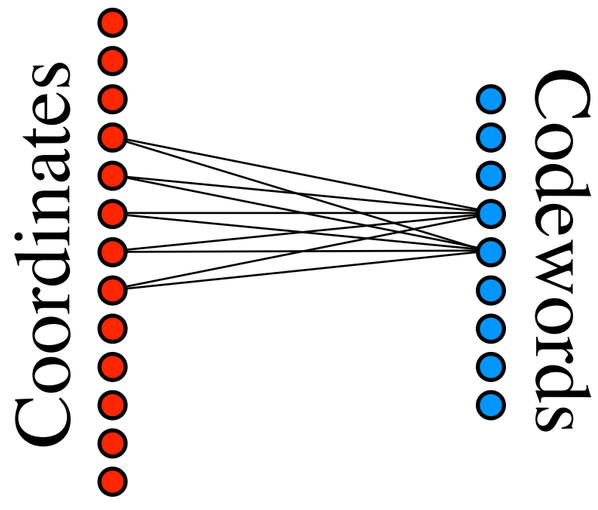
Probabilistic decoding

List-Decoding

Given e find all codewords of distance at most e.

Limits for RS-codes?

Johnson bound: If e is at most $1 - \sqrt{R}$ then the list size is $O(n)$.



Graph should not contain a $K_{k,2}$

Practical List-Decoding

Sudan, 1996: extend the WB-decoder!

Find

$$(h_0, h_1, \ldots, h_\ell) \in \mathbb{F}_q[x]_{<e} \times \mathbb{F}_q[x]_{<e+(k-1)} \times \cdots \times \mathbb{F}_q[x]_{e+\ell(k-1)}$$

not all zero, such that

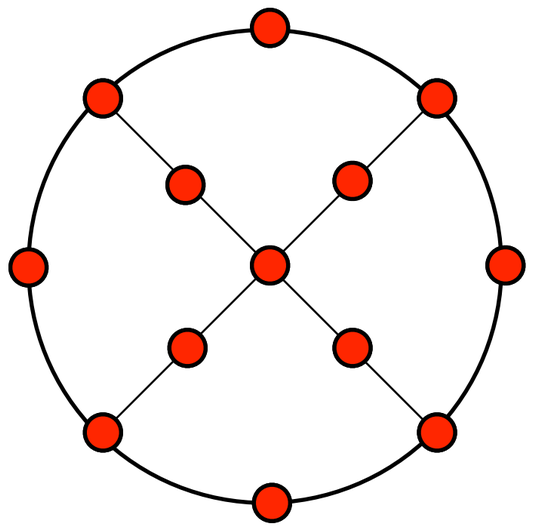
$$\forall\, i\colon \quad h_0(\alpha_i)y_i^\ell + h_1(\alpha_i)y_i^{\ell-1} + \cdots + h_\ell(\alpha_i) = 0$$

If number of correctly transmitted positions is $> e - 1 + \ell(k-1)$
then all correct polynomials *f* are *y*-zeros of

$$Q(x, y) = h_0(x)y^\ell + h_1(x)y^{\ell-1} + \cdots + h_\ell(x)$$

Example

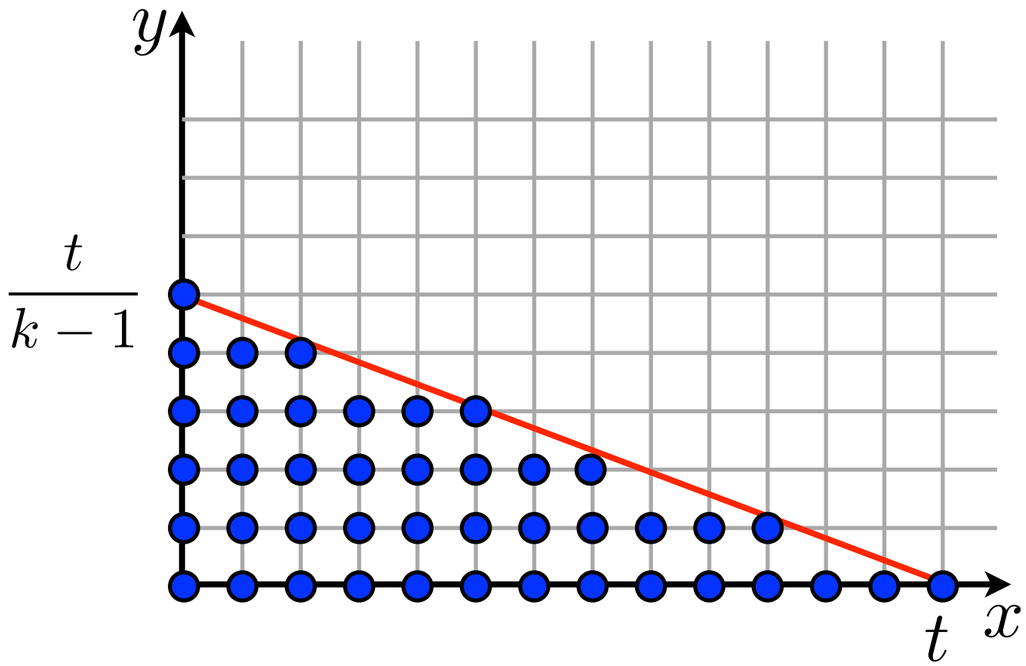
Find all lines that pass through at least 5 points:



$$Q(x,y) = x^4 - y^4 - 2x^2 + 2y^2$$

$$Q(x,y) = (x-y)(x+y)(x^2+y^2-2)$$

Analysis



t = number of correct positions

$(1, k-1)$-weighted degree of $Q < t$

Number of monomials in $Q > n$

Number of monomials in $Q \simeq \dfrac{t^2}{2k}$

$$t \simeq \sqrt{2kn}$$

Fraction of correctable errors $= 1 - \sqrt{2R}$

AG-Codes

This algorithm was generalized to the case of AG-codes by S-Wasserman.

The generalization introduced a “dictionary” with which generalizations of other types of algebraic algorithms were made possible.

Better Algorithm?

Guruswami-Sudan, 1998

We require that $Q(x, y)$ vanishes at (α_i, y_i) M times.

$$\text{Number of monomials} \simeq \frac{t^2}{2k} \qquad \Longrightarrow \quad t \simeq M\sqrt{kn}$$

$$\text{Number of constraints} \simeq \frac{M^2}{2} n$$

$\deg Q(x, f(x)) < t$

Each correct position contributes M zeros to $Q(x, f(x))$

If #correct positions $\cdot M > t$ then $Q(x, f(x)) = 0$

Fraction of correctable errors: $1 - \sqrt{R}$

Even Better?

Probably not with full length RS-codes (or AG-codes).

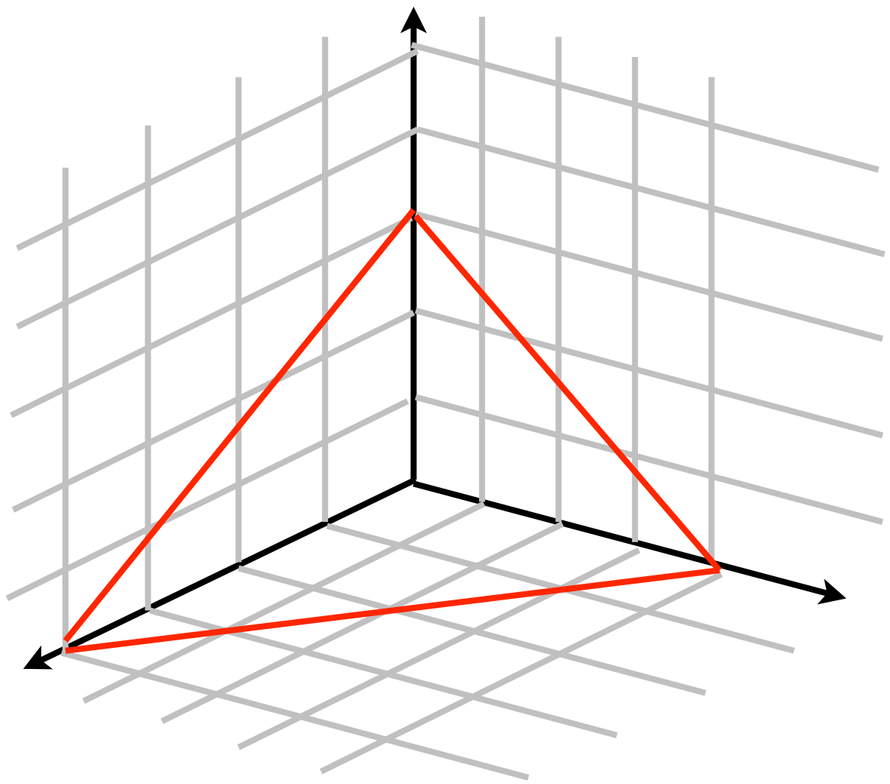
What if we use trivariate, or more generally m-variate polynomials?

Find polynomial $Q(x, y, z)$ of $(1, k-1, k-1)$ -weighted degree $< t$ such that

$$\forall\, i: \quad Q(\alpha_i, y_i, z_i) = 0$$

Even Better?

Parvaresh and Vardy



$$\text{Number of constraints} > n\frac{M^3}{6}$$

$$\text{Number of monomials in } Q \simeq \frac{t^3}{6k^2}$$

$$t \simeq M\sqrt[3]{nk^2}$$

errors are “interleaved”

If y_i and z_i are either both in error or both not in error, then for

$$\boxed{\text{fraction of errors} \leq 1 - R^{2/3}} \rightarrow 1 - R^{\frac{m-1}{m}}$$

then $Q(x, f(x), g(x)) = 0$. But what can be done with it?

Even Better?

Parvaresh and Vardy

Problem: only one polynomial relation.

Find another polynomial relation, and form the resultant of the multivariate polynomials.

Reduces to the old case if resultant nonzero.

Find Groebner basis of all the corresponding polynomials.

May not lead to the full decoding capability.

Probabilistic Algorithms?

Best fraction of errors to expect: $1 - R$

Assume that errors are "interleaved."

Coppersmith and Sudan: Correct a fraction of $1 - R - R\frac{m}{m+1}$ errors

with error probability $O\left(\frac{n^{O(m)}}{q}\right)$

Bleichenbacher et al.: Correct a fraction of $\frac{m}{m+1}(1 - R)$ errors

with error probability $O\left(\frac{n}{q}\right)$

Brown et al.: Correct a fraction of $\frac{m}{m+1}(1 - R) - \epsilon$ errors

with error probability $O\left(\frac{1}{q^{\epsilon n}}\right)$

Key Observation

Bleichenbacher et al.

If interleaved errors are assumed, then the error locator polynomial is the same for all the component codes.

Number of constraints: nm

Number of monomials: $(e+1)+m(e+k)=nm+1$

$$\Longrightarrow e=\frac{m}{m+1}(n-k)$$

Guarantees existence of nontrivial solution, but is that any good? (Probabilistic analysis)

AG-Codes

Brown et al.

All this (and more) can be generalized to AG-codes as well.

Can correct e errors with an error probability of

$$\left(\frac{1}{q-1}\right)^{\frac{m}{m+1}n(1-R)-\frac{2m-1}{m+1}g-\frac{m-1}{m+1}-e}$$

Algorithmic Issues

The matrix solution step can be done efficiently using the *displacement method*. (Olshevsky-S.)

The factorization step can be done efficiently using modifications of standard methods (Roth-Ruckenstein, Gao-S.)

All the algorithmic modifications can be generalized to AG-codes.

Further Results

The method of Guruswami-Sudan can be used to do soft-decision decoding of RS-codes (Koetter-Vardy).

Guruswami and co-authors have found a number of other codes which are list-decodable; it seems though that the list-decodability radius can only be increased when the alphabet size increases.

Still question remains whether the GS-bound can be improved for RS-codes (or even related codes).