Algebraic Geometric Codes

Without coding

M E S S A G E	→	M A S S A G E

With coding

M E S S A G E	→	M A S S A G E
M E S S A G E		M E S S A G E
M E S S A G E		M E S S A G E

Amin Shokrollahi

Bell Labs

Combinatorial Theory

Linear Codes

A linear code of block-length n and dimension k is a k-dimensional subspace of $\mathbb{F}_q^n$.

Its minimum distance d is the minimum Hamming distance between any two distinct elements.

$$[n, k, d]_q - \text{code}.$$

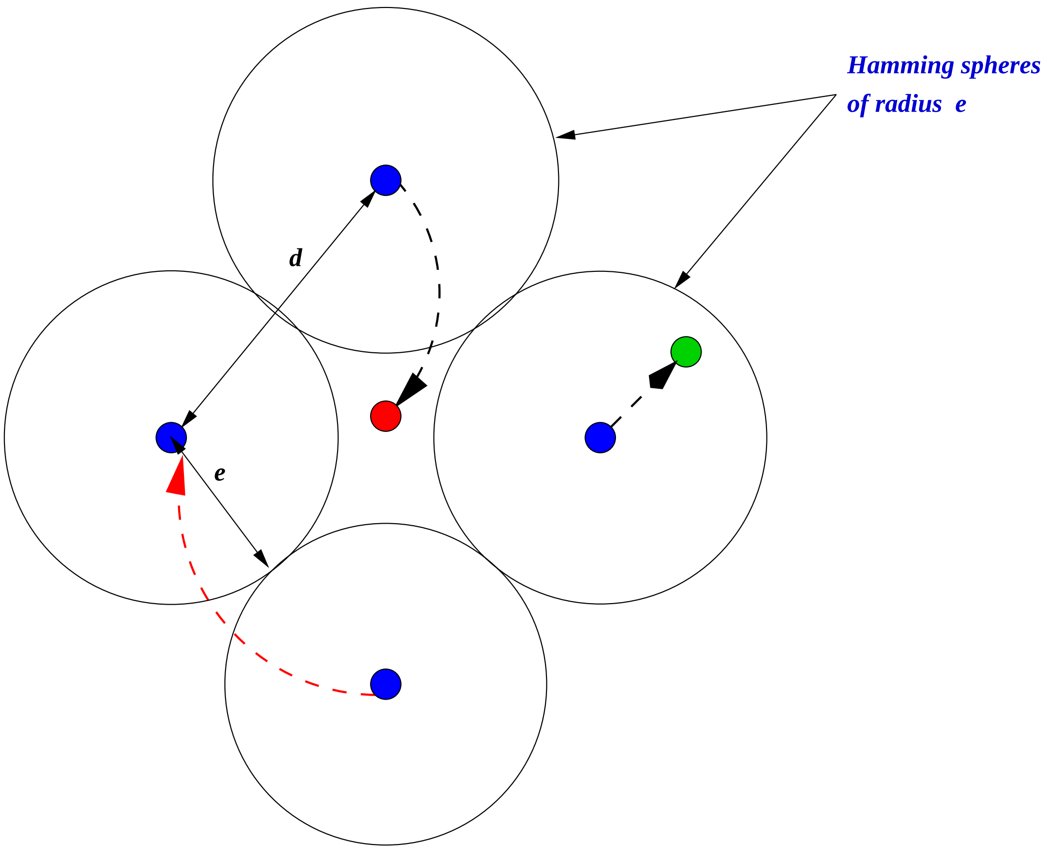
Linear Codes and Information Transmission

Fix a basis $\mathbf{v}_1, \ldots, \mathbf{v}_k$ for the code.

Encode a string $(b_1, \ldots, b_k) \in \mathbb{F}_q^k$ to codeword

$$b_1\mathbf{v}_1 + \cdots + b_k\mathbf{v}_k.$$

If code has minimum distance d, then one can decode to correct codeword if the number of errors is at most $(d-1)/2$.



Fundamental Question

Fix q.

For what values of n, k, and d does there exist an $[n, k, d]_q$-code?

Answer is HARD in general!

Asymptotic statements?

Asymptotic Analysis

A sequence of $[n_\ell, k_\ell, d_\ell]_q$-codes such that $n_\ell \to \infty$ and $k_\ell/n_\ell \to R > 0$ and $d_\ell/n_\ell \to \delta > 0$ is called asymptotically good.

Relaxation of the fundamental question: what is the shape of the point set (δ, R)?

Asymptotic Bounds

Singleton-bound:
for any $[n,k,d]_q$-code we have

$$k + d \leq n + 1.$$

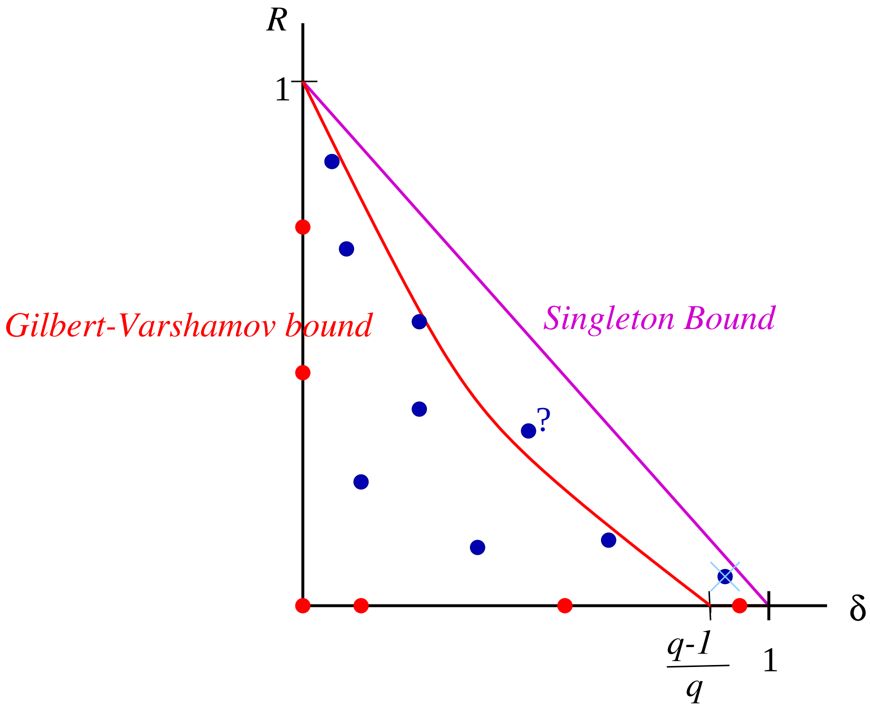
This shows that $R + \delta \leq 1$.

Gilbert-Varshamov bound:
There are sequences of codes such that

$$R \geq 1 - H_q(\delta)$$

for $0 \leq \delta \leq (q-1)/q$, where

$$H_q(x) = x \log_q(q-1) - x \log_q(x) - (1-x) \log_q(1-x).$$



Singleton Bound

Are there codes that achieve equality in the Singleton bound, i.e., $[n, k, d]_q$-codes such that $d + k = n + 1$?

Yes!

Reed-Solomon Codes

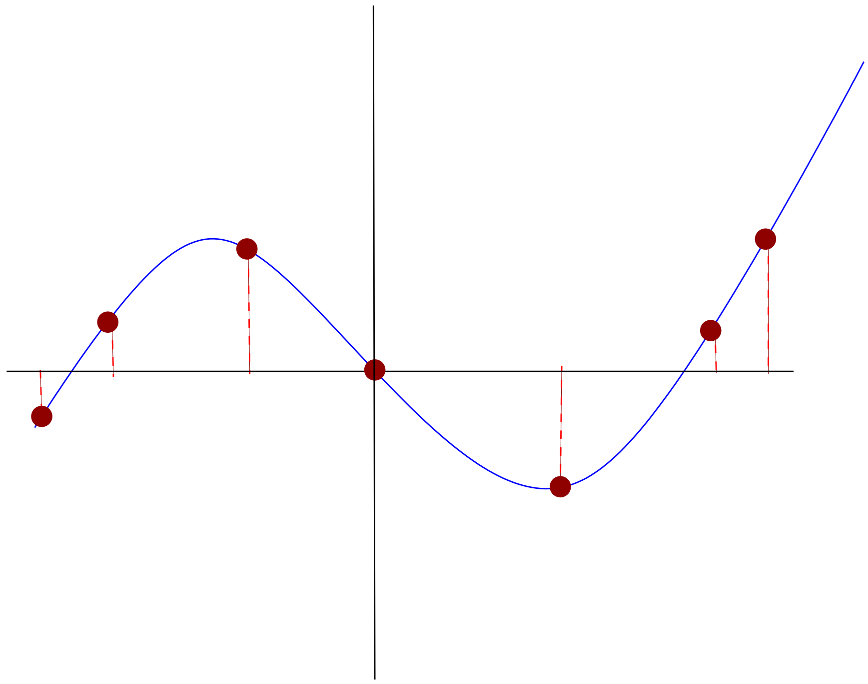
Take n distinct elements $x_1, \ldots, x_n$ in $\mathbb{F}_q$.

The code is the image of the linear map

$$\begin{array}{rcl} \mathbb{F}_q[x]_{<k} & \to & \mathbb{F}_q^n \\ f(x) & \mapsto & (f(x_1), \ldots, f(x_n)). \end{array}$$

So: code consists of evaluation of bounded degree polynomials.

Dimension and minimum distance?



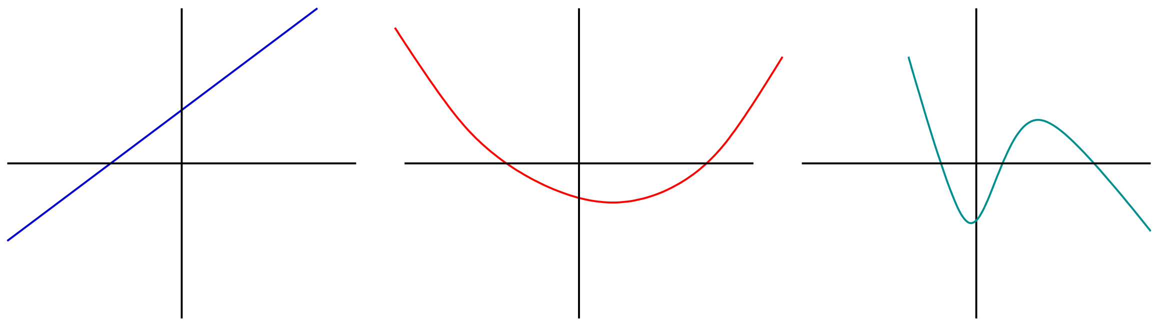
An old Friend

Polynomial of degree less than k over a field can have at most $k-1$ zeros over that field.

If $k \leq n$, then the evaluation map is injective, hence dimension of the code is k.

Number of zero coordinates of a nonzero codeword is at most equal to $k-1$, hence minimum distance is at least $n-k+1$.

Singleton bound shows that minimum distance equals $n-k+1$.



Consequences

For the code we need distinct elements $x_1, \ldots, x_n$.

Hence, $n \leq q$, i.e., for fixed q we cannot construct arbitrarily long such codes.

Generalizations

Evaluate at all points $(\alpha, \beta) \in \mathbb{F}_q^2$ in the plane.

Define the code as the image of the evaluation map

$$\begin{array}{rcl} \mathbb{F}_q[x,y]_{<\ell,<\ell} & \to & \mathbb{F}_q^n \\ f(x) & \mapsto & (f(\alpha,\beta) \mid \alpha,\beta \in \mathbb{F}_q). \end{array}$$

Dimension of the code is ℓ^2.

Minimum distance is at least $q^2 - 2(\ell - 1)q$ by the Schwartz-Zippel Lemma.

In general, one has a code of dimension ℓ^m and minimum distance at least $q^m - m(\ell - 1)q^{m-1}$.

For $m \to \infty$, the rate $(\ell/q)^m$ converges to 0.

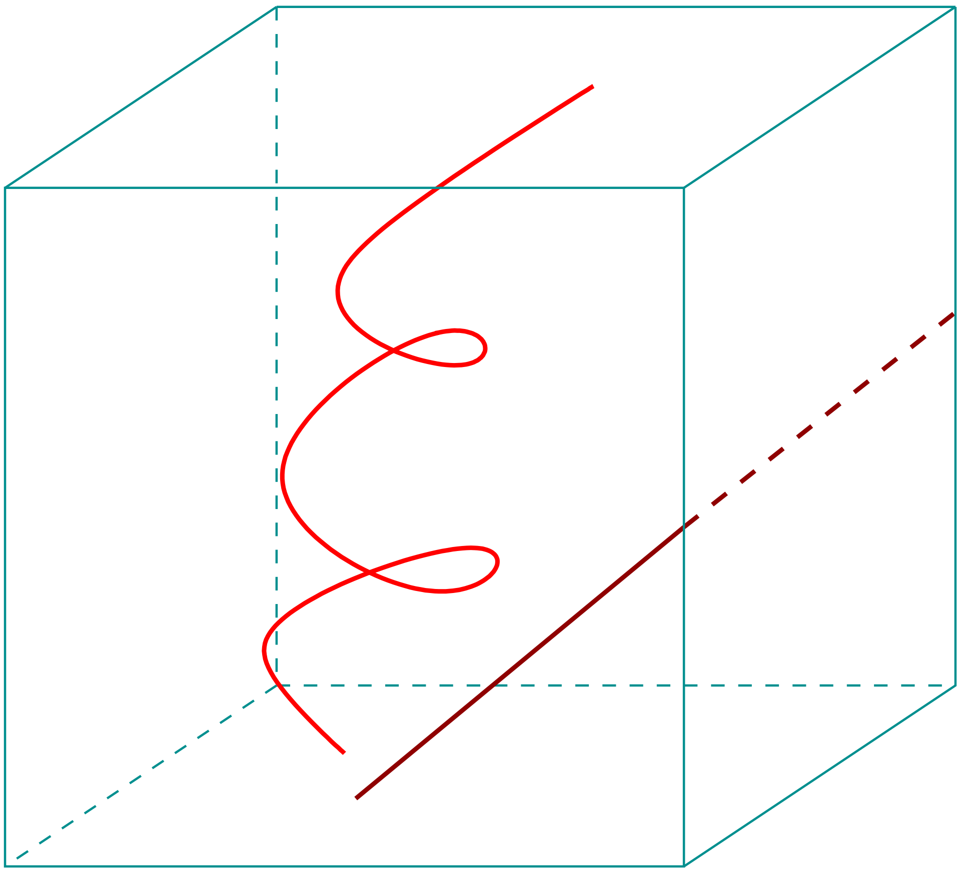
AG-Codes

Point Sets

The Schwartz-Zippel Lemma only holds for point sets of the form H^m.

What if we choose the evaluation points in a more clever way?

We could, for instance, choose them on a curve.



AG-Codes - History

- Goppa'70: Classical Goppa codes.
- Goppa'81: Algebraic-geometric codes (geometric Goppa codes).
- Tsfasman, Vladut, Zink'82: Codes above the Gilbert-Varshamov bound.

Example

Points $(\alpha, \beta) \in \mathbb{F}_{13}^2$ such that $\beta^2 = 2\alpha^3 + 11\alpha$. (19 points.)

Polynomials: $\langle 1, x, y, x^2, xy, x^3 \rangle$.

Dimension and Minimum distance:

$(f_0 + f_1 x + f_2 x^2 + f_3 x^3) + y(g_0 + g_1 x) =: F(x) + yG(x)$.

$F(x) + yG(x)$ vanishes at (α, β) iff $F(x) - yG(x)$ vanishes at $(\alpha, -\beta)$.

Number of zeros of

$$F(x)^2 - y^2 G(x)^2 = F(x)^2 - (2x^3 + 11x) G(x)^2$$

is at most 6.

Number of zeros of $F(x) + yG(x)$ is at most 6.

This gives a

$$[19, 6, 13]_{13} - \text{code}.$$

Exact Description

Interpret x_i as points on the projective line over $\mathbb{F}_q$. Then $\mathbb{F}_q[x]$ is the ring of all functions having a pole only at ∞, and $\mathbb{F}_q[x]_{<k}$ is the $\mathbb{F}_q$-space of all functions having only a pole at ∞ of order less than k.

Let $\mathcal{X}$ be an absolutely irreducible algebraic curve over $\mathbb{F}_q$, let $Q, P_1, \ldots, P_n$ be $\mathbb{F}_q$-rational points of $\mathcal{X}$, and let α be an integer.

$L(\alpha Q)$ is the $\mathbb{F}_q$-space of all functions on $\mathcal{X}$ having poles only at Q of order at most α. Define

$$\gamma\colon L(\alpha Q) \to \mathbb{F}_q^n, \quad f \mapsto (f(P_1), \ldots, f(P_n)).$$

Image of γ is a linear code of block-length n over $\mathbb{F}_q$.

Parameters of AG-Codes

Theorem. Number of poles of a nonzero function f on $\mathcal{X}$ equals number of zeros of f (counted with multiplicities).

Implies that $\dim C = \dim L(\alpha Q)$.

Implies that minimum distance of C is at least $n - \alpha$.

Theorem of Riemann. $\dim L(\alpha Q) \geq \alpha - g + 1$, where g is the genus of $\mathcal{X}$.

Implies that $\dim(C) \geq \alpha - g + 1$.

General Case

Given algebraic curve $\mathcal{X}$, we obtain

$$[n, k, \geq n - k - g + 1]_q - \text{code},$$

where g is the genus of the curve.

These curves will asymptotically give

$$R + \delta \geq 1 - \frac{g}{n}$$

Need fraction g/n as small as possible.

The quantity

$$d^* := n - k - g + 1$$

is called the designed distance of the code.

Asymptotically good Codes

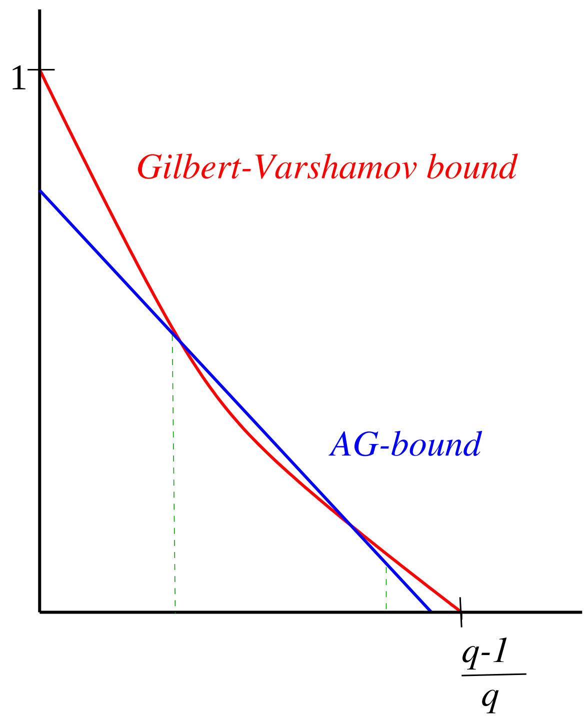
(Tsfasman, Vladut, and Zink'82)

If q is a square, then one can construct sequences of curves $\mathcal{X}_\ell$ of genus g_ℓ and n_ℓ points over $\mathbb{F}_q$ such that

$$\frac{g_\ell}{n_\ell} \to \frac{1}{\sqrt{q}-1}$$

as ℓ goes to ∞. (Modular curves.)

If $q \geq 49$ is a square, then we obtain codes that are better than the Gilbert-Varshamov bound!

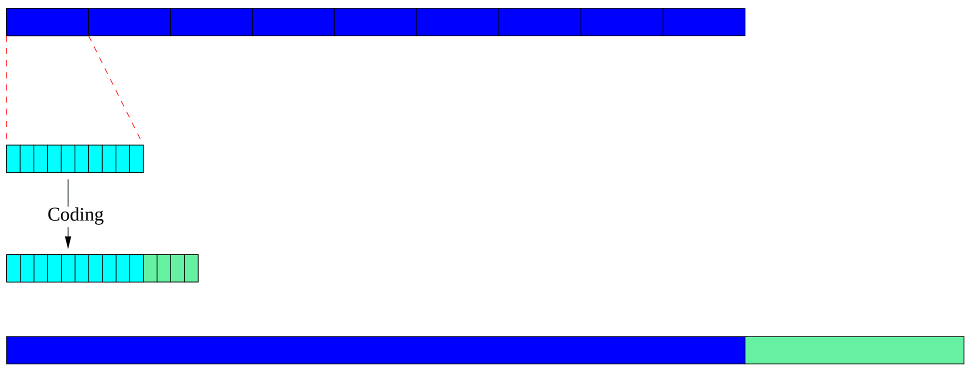


Binary Codes

(Barg, Katsman, and Tsfasman '87)

There are no good binary AG-codes known.

Use concatenation: $[91, 24, 25]_2$-code. World record!



Decoding

History

- Driencourt'86: decoding up to $(d^* - 1)/4$ for elliptic curves.

- Justesen, Larsen, Elbrønd Jensen, Havemose, Høholdt'
Decoding up to $(d^* - 1)/2 - g/2$ for plane algebraic curves.

- Skorbogatov-Vladut'90: generalization to arbitrary curves.

- Duursma'93: $(d^* - 1)/2 - \sigma$ (extended algorithm).

- Pellikaan'89: $(d^* - 1)/2$ for certain curves, theoretical algorithm. Generalized by Vladut'90.

- Porter, Shen, Pellikaan'92: $(d^* - 1)/2 - \sigma$, different algorithm.

- Ehrhard'93: Decoding up to $(d^* - 1)/2$.

- Ehrhard'93, Feng-Rao'93+Duursma'93: Decoding up to $(d^* - 1)/2$ (and sometimes beyond) via majority vote.

- Sudan'95 List decoding of Reed-Solomon codes.

- S-Wasserman'97 List decoding of AG-codes.

- Guruswami-Sudan'98 improvements.

Decoding Reed-Solomon Codes

Bounded Distance Decoding

Given $(y_1, \ldots, y_n)$ and a promise that it has Hamming distance $\leq (n-k)/2$ to a Reed-Solomon code of dimension k, find the closest codeword.

Solution (Berlekamp-Welch'83):

Compute polynomials

$$h \in \mathbb{F}_q[x]_{\leq (n-k)/2} \text{ and } g \in \mathbb{F}_q[x]_{<(n+k)/2},$$

not both zero, such that

$$\forall\, i = 1, \ldots, n: \qquad g(x_i) + y_i h(x_i) = 0.$$

Then $f := g/h$ is a polynomial and the closest codeword is the evaluation of this polynomial at $x_1, \ldots, x_n$.

Why?

This is why!

(1) Existence of g and h: number of unknown coefficients is $(n-k)/2+1+(n+k)/2 = n+1$, number of equations is n.

(2) Let closest codeword be the evaluation of polynomial u of degree $< k$. Let $H(x) := g(x) + u(x)h(x)$. Then

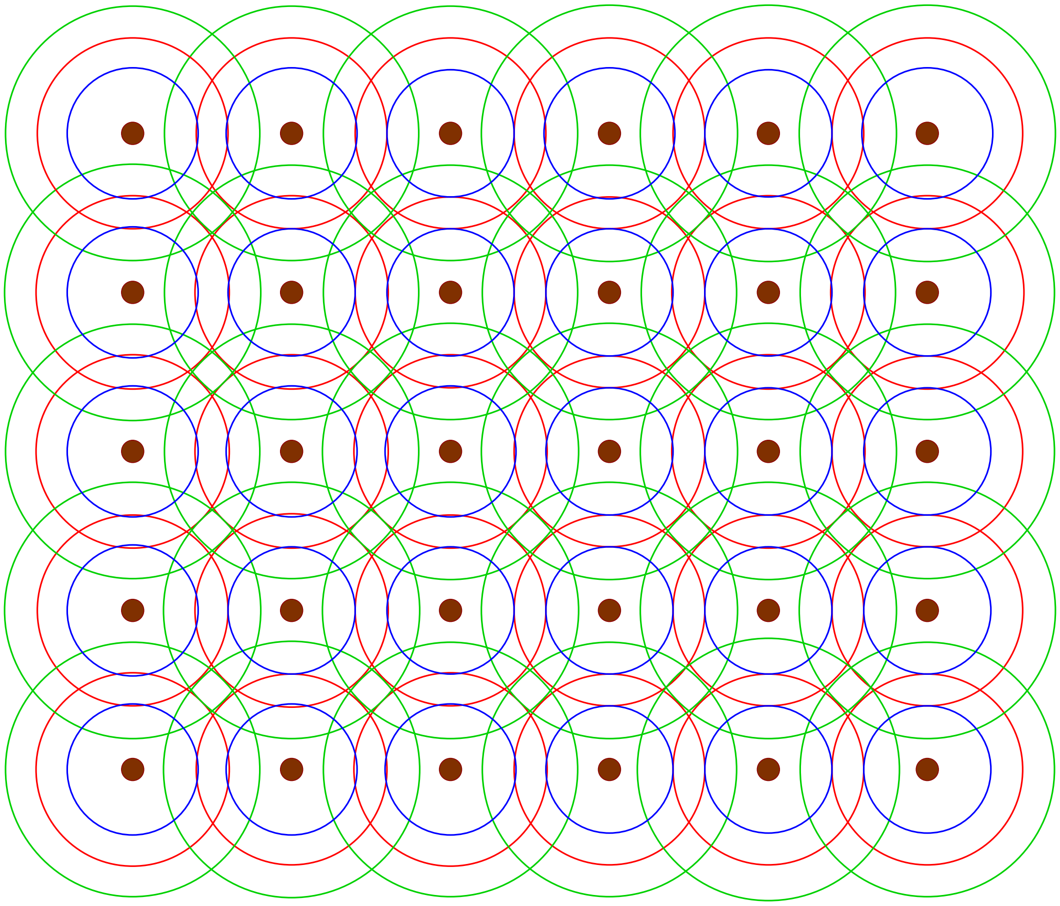
$$H(x_i) = g(x_i) + y_i h(x_i) = 0 \text{ iff } u(x_i) = y_i.$$

Number of such i is number of correct coordinate places, i.e., at least $n-(n-k)/2 = (n+k)/2$.

Hence, H has at least $(n+k)/2$ roots; but its degree is less than $(n+k)/2$, so $H = 0$.

List Decoding

Increase the error-radius and decode to obtain a list of possible codewords.



List Decoding Reed-Solomon Codes – Sudan'95

Given $(y_1, \ldots, y_n)$ and a promise that it has Hamming distance $\leq e$ to a Reed-Solomon code of dimension k, find a list of codewords of distance $\leq e$.

Solution:

Compute polynomials

$$h_0, h_1, \ldots, h_\ell \in \mathbb{F}_q[x] \text{ of appropriate degrees}$$

not all zero, such that

$\forall\, i = 1, \ldots, n$: $\quad h_0(x_i) + h_1(x_i)y_i + \cdots + h_\ell(x_i){y_i}^\ell = 0.$

Then codewords of distance $\leq e$ are evaluations of polynomials f satisfying

$$h_0(x) + h_1(x)f + \cdots + h_\ell(x)f^\ell = 0.$$

Why....

Decoding AG-Codes – S&Wasserman'97

Recall the code obtained by evaluation of

$$\langle 1, x, y, x^2, xy, x^3 \rangle$$

at the points of $y^2 = 2x^3 + 11x$ over $\mathbb{F}_{13}$. We want to decode

$$z = (0, 9, 9, 5, 1, 6, 6, 0, 3, 10, 1, 1, 2, 3, 6, 8, 3, 6, 12)$$

to codeword of distance ≤ 5.

First step: find

$$g \in \langle 1, x, y, x^2, \ldots, x^6, x^5 y \rangle$$

and

$$h \in \langle 1, x, y, \ldots, x^3, x^2 y \rangle$$

such that

$$\forall\, i = 1, \ldots, 19: \quad g(x_i, y_i) + h(x_i, y_i) z_i = 0.$$

This results in finding nonzero element in the kernel of

1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	0	1	0	1	0	1	0	1	0	1	0	9	9	0	9	0	9	0
1	12	0	1	0	12	0	1	0	12	0	1	0	9	4	0	9	0	4	0
1	11	1	4	11	5	4	3	5	7	3	12	7	5	3	5	7	3	12	7
1	6	2	10	12	8	7	9	3	2	5	12	4	1	6	2	10	12	8	7
1	10	2	9	7	12	5	3	11	4	6	1	8	6	8	12	2	3	7	4
1	3	3	9	9	1	1	3	3	9	9	1	1	6	5	5	2	2	6	6
1	7	3	10	8	5	4	9	2	11	1	12	7	0	0	0	0	0	0	0
1	4	4	3	3	12	12	9	9	10	10	1	1	3	12	12	9	9	10	10
1	2	5	4	10	8	7	3	1	6	2	12	4	10	7	11	1	9	2	5
1	9	6	3	2	1	5	9	6	3	2	1	5	1	9	6	3	2	1	5
1	9	7	3	11	1	8	9	7	3	11	1	8	1	9	7	3	11	1	8
1	2	8	4	3	8	6	3	12	6	11	12	9	2	4	3	8	6	3	12
1	4	9	3	10	12	1	9	4	10	3	1	12	3	12	1	9	4	10	3
1	3	10	9	4	1	12	3	10	9	4	1	12	6	5	8	2	11	6	7
1	7	10	10	5	5	9	9	11	11	12	12	6	8	4	2	2	1	1	7
1	6	11	10	1	8	6	9	10	2	8	12	9	3	5	7	4	3	11	5
1	10	11	9	6	12	8	3	2	4	7	1	5	6	8	1	2	10	7	9
1	11	12	4	2	5	9	3	8	7	10	12	6	12	2	1	9	11	8	4

We find

$$g = 6x^6 + x^5 + 4x^4 + (4y+7)x^3 + (y+9)x^2 + (3y+12)x,$$

and

$$h = x^3 + x^2 + 4x + (5y+7)$$

Second Step: Calculate $f = g/h$ and evaluate at all points:

We find

$$f = 2x + 5x^2 + 7x^3$$

which gives codeword

$$(0, 1, 9, 12, 1, 6, 6, 8, 3, 2, 1, 1, 2, 3, 6, 8, 1, 6, 12)$$

List Decoding AG-Codes – S&Wasserman'97

Is analogous to list decoding of RS-codes.

List Decoding is reduced to

- Solving a homogeneous system of linear equations.

- Finding roots of a polynomial over a function field.

List Decoding – Results

Decoding with lists of polynomial size possible in polynomial time if number of errors is at most

$$1 - \sqrt{2R + 2\frac{g}{n}} - \frac{g}{n}$$

This bound has been recently improved to

$$1 - \sqrt{R + \frac{g}{n}}$$

by Guruswami&Sudan'98.

Efficiency Issues

- Berlekamp-Welch decoder for RS-codes:$O(n^2)$.

- Efficient AG-decoders: Justesen, Larsen, Jensen, Høholdt'92, Shen'93, Sakata, Justesen, Madelung, Jensen, Høholdt'95 (and subsets thereof), $O(n^{7/3})$.

- Sudan's algorithm: $O(n^6)$

- Generalization by S&Wasserman: $O(n^8)$.

- Efficient root finders (S-Gao): $O(n^2\ell)$

- Efficient version of Sudan's algorithm (Roth-Ruckenstein'98): $O(n^2\ell)$.

- Displacement-structure approach (Olshevsky-S): $O(n^2\ell)$ for RS-codes and $O(n^{7/3}\ell)$ for AG-codes; Parallel algorithms.